RASFinder™
Remote Access Device

Remote Access Server with Integrated WAN Devices

Model MTASR3-200

User Guide

MultiTech® Systems

User Guide

S0000055 Revision E

RASFinder (Model No. MTASR3-200)

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 2004-07, by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Description
A (3/23/98)	Manual released. All pages at revision A.
B (1/26/99)	Manual revised to include software revision 3.00. All pages at revision B.
C (3/19/01)	Manual revised to include software revision 3.10. All pages at revision C.
D (4/13/04)	Manual updated to remove coax cable connector and include latest software.
E (8/02/04)	Manual updated to include a new version of WINMCSI2000 and XP.
F (6/20/07)	Updated the Technical Support contact list and warranty statement and corrected the pin out for the command cable. Updated CD image.

Patents

This Product is covered by one or more of the following U.S. Patent Numbers: **5.301.274; 5.309.562**; **5.355.365; 5.355.653; 5.452.289; 5.453.986**. Other Patents Pending.

TRADEMARK

Multi-Tech and the Multi-Tech logo are registered trademarks of Multi-Tech Systems, Inc. RASFinder is a trademark of Multi-Tech Systems, Inc.

Adobe Acrobat is a trademark of Adobe Systems Incorporated.
K56flex is a trademark of Rockwell International Corporation and Lucent Technologies Corporation.
Microsoft Windows, Windows 98, 2000, XP and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112 U.S.A
Telephone: (763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Internet Address: http://www.multitech.com

Contents

Chapter 1 - Introduction and Description 5

Introduction 6
- Preview of this Guide 6

Front Panel 8

Back Panel 9
- Link Connectors (Links 1, 2, and 3) 9
- Ethernet 10Base-T Connector 9
- Command Connector 9
- Power Connector 9

Specifications 10
- Ethernet Port 10
- Command Port 10
- WAN Links 10
- Electrical/Physical 10
- Requirement 10

Chapter 2 - Installation 11

Introduction 12

Unpacking 12

Safety Warning Telecom 12

Cabling Your RASFinder 13

Adding RAM 14

Chapter 3 - Software Loading and Configuration 15

Installing Your RASFinder Software 16
- IPX Routing Setup 19
- IP Routing Setup 19

Setting Up Your Remote User Database 22

Setting Up Remote Access Dial In User Server (RADIUS) 27

Final Routing Setup 29

Chapter 4 - RASFinder Software 32

Introduction 33

Before You Begin 33

RASFinder Setup 34

Typical Applications 35
- RAS Applications 35
- Router Application 41

IP Setup 44
- Filters 49

IPX Setup 51
- Bandwidth Optimization Group 52
- IPX Filters 53

Spanning Tree Setup 54

WAN Port Setup 56

Point-to-Point Setup 57

Applications 58

Diagnostics 58

Client 59

Chapter 5 - RAS Dial-Out Redirector 60
Introduction 61
Installing and Configuring the WINMCSI Modem-Sharing Software 61
Running the WINMCSI Workstation Software 64

Chapter 6 - Remote Configuration and Management 67
Introduction 68
Remote Configuration 68
Modem-Based 68
LAN-Based 70
Remote Management 72
Telnet 72
Web Browser Management 75

Chapter 7 - Service, Warranty and Tech Support 76
Introduction 77
Limited Warranty 77
On-line Warranty Registration 77
Service 78
U.S. and Canadian Customers 78
International Customers (outside U.S.A. and Canada) 78
International Distributors 79
Replacement Parts 79
Technical Support 79
Internet Sites 79

Appendixes 80
Appendix A - Cabling Diagrams 81
Appendix B - Script Language 82
Appendix C - Regulatory Information 84
Class B Statement 84
Fax Branding Statement 84
FCC Part 68 Telecom 85
Ringer Equivalence Number 86
EMC, Safety and Terminal Directive Compliance 86
Appendix D - AT Command Summary 87
Appendix E - TCP/IP 94
TCP/IP 94
Internet Protocol (IP) 96

Glossary of Terms 97

Index 111

RASFinder™
Remote Access Device

Chapter 1 - Introduction and Description

MultiTech® Systems

Introduction

Welcome to Multi-Tech's new RASFinder™ Model MTASR3-200, a Remote Access Server (RAS) for remote dial-in access and LAN-to-LAN routing capability. The RASFinder 200-Series is a remote access device that supports up to three concurrent dial-in sessions and IP or IPX remote access. The RASFinder 200-Series features a 10Base-T port for local LAN connection, Command port for configuration, and three internal V.90 modems. New features include additional security using Multi-Tech's Remote Dial In User Server (Radius), support for Simple Network Time Protocol (SNTP) clocking, and added security for remote dial-in users. System management is provided through the Command port using bundled Windows® based software which provides easy-to-use configuration menus.

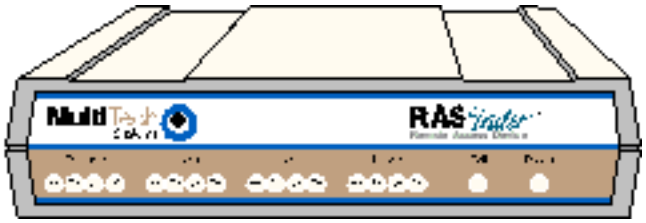


Figure 1-1. RASFinder

Note: Though the modems in the RASFinder are capable of 56 Kbps download performance, line impairments, public telephone infrastructure, and other external technological factors currently prevent maximum 56 Kbps connections.

Preview of this Guide

This guide describes the RASFinder and tells you how to install and configure the unit. The information contained in each chapter is as follows:

Chapter 1 - Introduction and Description

This chapter describes the RASFinder 200-Series Remote Access Server with integrated WAN devices. Descriptions of the front panel indicators and back panel connectors and switch are provided. A list of relevant specifications is provided at the end of the chapter.

Chapter 2 - Installation

This chapter provides information on unpacking and cabling your RASFinder. The installation procedure describes each cable connection starting with connecting the power cord, Command port, LAN and finally the WAN. The software installation process must be done through the MTASR3-200 Command port.

Chapter 3 - Software Loading and Configuration

Chapter 3 details the software loading and initial configuration. Initially, the RASFinder software configures the unit for a Remote Access Server (RAS) configuration. If you want to configure the RASFinder for a Lan-to-Lan configuration, you will have to change the Remote Port Setup to a Client or LAN setting. The RASFinder can also be configured to operate in either a RAS application using a Radius server for security services or a RAS application using the proprietary Remote User Data Base Utility for remote user authentication.

Chapter 4 - RASFinder Software

Chapter 4 describes the RASFinder software designed for the Windows® environment. The software contains a number of utilities that allow for downloading updated firmware, creating a proprietary Remote User Data Base, and a terminal emulation utility for configuring the internal modems. Three typical applications are provided to show you how the RASFinder can be configured and some insight into the application.

Chapter 5 - RAS Dial-Out Redirector

Chapter 5 describes how Multi-Tech's Remote Access Server for Microsoft network users enables them to dial out and fax out through the MTASR3-200. It provides information on installing and configuring the WINMCSI modem-sharing software.

Chapter 6 - Remote Configuration and Management

This chapter provides procedures for changing the configuration of a remote RASFinder located elsewhere on a LAN or at the other end of a modem connection. This chapter also describes typical Telnet client and Web-browser management of the RASFinder.

Chapter 7 - Service, Warranty and Tech Support

This chapter provides statements concerning the product warranty, provides space for recording information about your RASFinder prior to calling Multi-Tech's Technical Support, and includes instructions for contacting Technical Support and returning your RASFinder to the factory if it requires service. Also included is information on how to obtain product support through the Internet.

Front Panel

The front panel has four groups of LEDs that provide the status of the LAN connection and link activity. Two other LEDs indicate the general status of the RASFinder. The Ethernet LEDs display the activity of the LAN, i.e., whether the RASFinder is connected to the LAN, transmitting or receiving packets, or if a collision is in progress. The Link LEDs display the status of the three links that can be connected to the RASFinder and show whether a link is ready to transmit or receive serial data. The last two LEDs indicate whether the self-test passed or failed and if the power ON/OFF switch on the back of the RASFinder is set to ON.

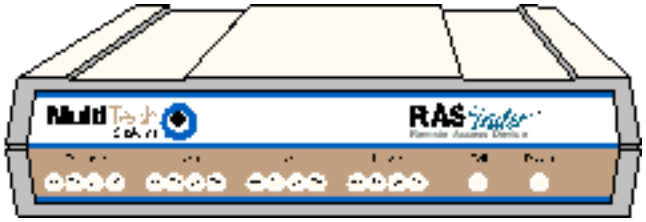


Figure 1-2. Front Panel

ETHERNET

RD Receive Data indicator blinks when packets are being received from the local area network.

TD Transmit Data indicator blinks when packets are being transmitted to the local area network.

CL Collision indicator lights when a collision is in progress; that is, when two nodes are transmitting packets at the same time.

LK Link indicator lights indicating that the RASFinder is connected to the local area network.

LINK x

RD Receive Data indicator blinks when the link is receiving data.

TD Transmit Data indicator blinks when the link is transmitting data.

CD Carrier Detect indicator lights when the link detects a carrier signal.

TR Terminal Ready indicator blinks when the link is ready to transfer data.

Fail Fail indicator lights for 2 minutes when power is applied to the RASFinder; if it remains on for over 3 minutes, it indicates that a boot failure has occurred.

Power The power indicator lights when the On/Off Switch is in the ON position.

Back Panel

The cable connections for the RASFinder are made on the back panel. Three groups of cables are used on the RASFinder: the Command port, three RJ-11 ports (Links 1, 2, and 3), and the Ethernet port. The cable connections are shown in Figure 1-3 and defined in the following groups.

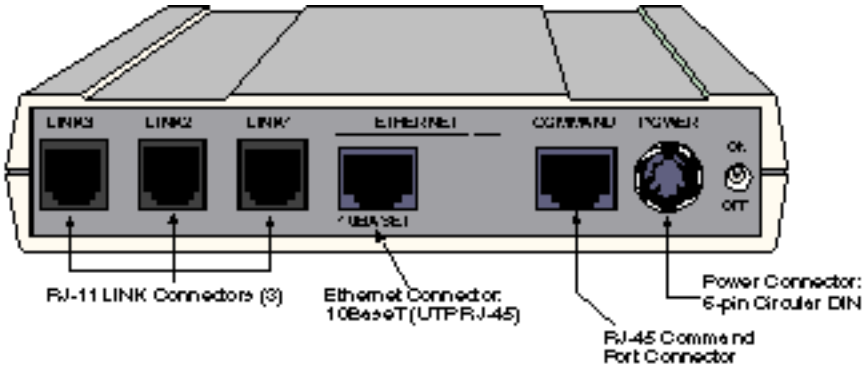


Figure 1-3. Back Panel

Link Connectors (Links 1, 2, and 3)

These Link connectors are used to connect the RASFinder to a WAN. These connectors are RJ-11 connectors.

Ethernet 10Base-T Connector

The Ethernet 10Base-T connector is used to connect the RASFinder to a LAN using unshielded twisted cable. This connector is an RJ-45 jack.

Command Connector

The Command connector is used to configure the RASFinder using a PC with a serial port and running Windows® software. The Command connector is an RJ-45 jack and a short adapter cable is provided to convert to a standard serial port DB25 female connector.

Power Connector

The Power connector is used to connect the external power supply to the RASFinder. The Power connector is a 6-pin circular DIN connector. A separate power cord is connected to the power supply and the live AC grounded outlet.

Specifications

The RASFinder conforms to the following specifications:

- Routing Protocols - IP and IPX, and bridging for all others
- Ethernet LAN Interface - 10Base-T (twisted pair)
- WAN Interface - 3 async (RS232) Links with RJ-11 jacks
- Command Port - 19.2 Kbps Asynchronous
- Two 70-nanosecond 4 MB SIMMs (8 MB, total)
  (RAM is expandable to a maximum of 32 MB)
  Caution: SIMM speed and size cannot be mixed.
- 1 MB of Flash memory (on two PROMs)

Ethernet Port

- One Ethernet Interface - 10Base-T (twisted pair) RJ-45 connector.

Command Port

- Single 19.2 Kbps asynchronous Command Port using a short RJ-45-to-DB9 cable with a DB9 female connector.

WAN Links

- Three internal V.90 modems* with MultiLink Point-to-Point Protocol for a bandwidth of up to 168 Kbps.

Electrical/Physical

- Voltage - 100 to 250 VAC, 50/60 Hz
- Input Voltage - 5Vdc, 1.4A
- Power Consumption - 10 Watts
- Dimensions - 1.625" high x 6" wide x 9" deep

  5.63 cm high x 22.34 cm wide x 33.51 cm deep
- Weight - 2 pounds (0.92 kg)

Requirement

- PC with Windows 98/2000/XP or Windows NT, and one available serial COM port to connect to the Command Port of the RASFinder

* Though this modem is capable of 56 Kbps download performance, line impairments, public telephone infrastructure and other external technological factors currently prevent maximum 56 Kbps connections.

RASFinder™
Remote Access Device

Chapter 2 - Installation

MultiTech® Systems

Introduction

This chapter is organized to provide instructions for unpacking and cabling your RASFinder. The unpacking section describes the contents of the shipping box and shows how the RASFinder is packaged. The installation procedure describes each cable connection and shows where that cable is connected to the RASFinder. If additional RAM is needed on your RASFinder, a detailed procedure is provided describing how to install a second SIMM.

Unpacking

The shipping box contains the RASFinder, external power supply, a plastic bag containing cables, RASFinder CD with the RASFinder Software, Quick Start, and User Guide in Adobe Acrobat™ format. Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the unit; contact Multi-Tech's Technical Support for advice (refer to Chapter 7). If no damage is observed, place the RASFinder in its final location and perform the procedures in the section on "Cabling Your RASFinder."

Save the shipping box in case reshipment is necessary.

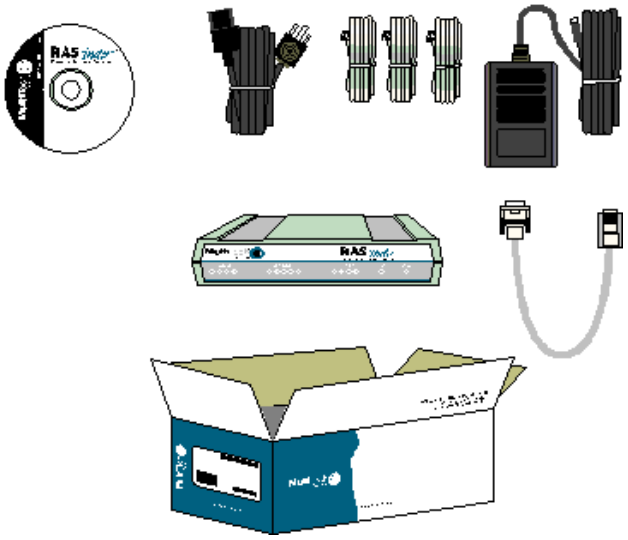


Figure 2-1. Unpacking

Safety Warning Telecom

1. Never install telephone wiring during a lightning storm.
2. Never install a telephone jack in wet locations unless the jack is specifically designed for wet locations.
3. This product is to be used with UL and cUL listed computers.
4. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
5. Use caution when installing or modifying telephone lines.
6. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
7. Do not use the telephone to report a gas leak in the vicinity of the leak.
8. To reduce the risk of fire, use only 26 AWG or larger telecommunication line cord.

Cabling Your RASFinder

Cabling your RASFinder involves making the proper WAN, Ethernet, Command port, and Power connections. Should you need to install additional RAM, or replace a SIMM module some time in the future, refer to the next section on “Adding RAM”.

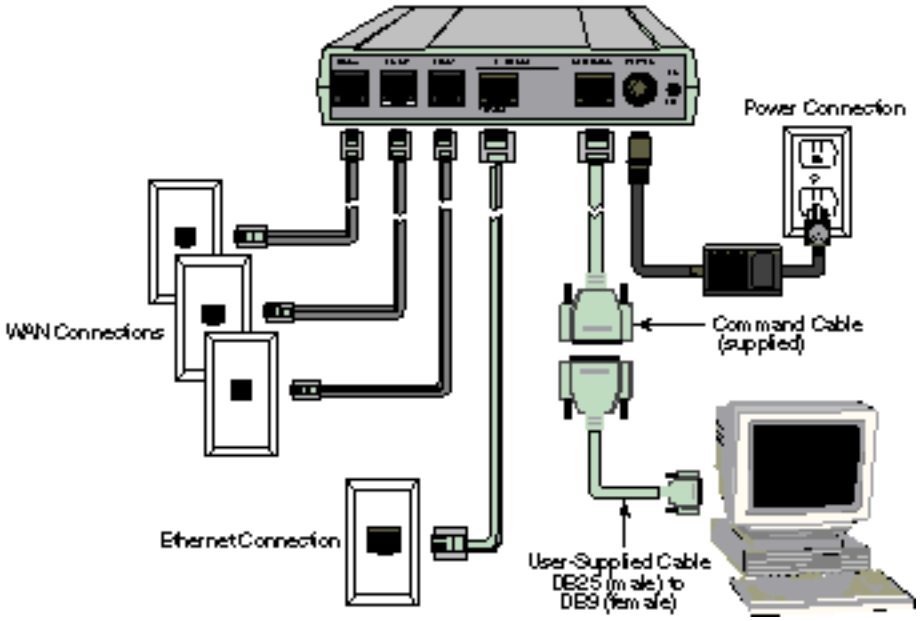


Figure 2-2. Back Panel Connections

Note: If additional RAM is needed, perform the procedure in the next section, “Adding RAM”.

The following steps detail the procedures for connecting the cables to your RASFinder.

1. Connect the RASFinder to a PC Comm port using the short RJ-45 to DB9 (female) cable (provided). Plug the RJ-45 end of the Command cable into the Command port of the RASFinder, then connect the DB9 (female) connector to the PC's serial port. See Figure 2-2.
2. Connect either an RJ-45 (UTP) cable to the 10 BASE-T connector on the back of the RASFinder. Connect the other end of the cable to your LAN.
3. Connect one end of an RJ-11 cable to each of the LINK Connectors on the RASFinder (labeled LINK 1, LINK 2, and LINK 3) and connect the other end to the phone jacks (shown in Figure 2-2).
4. Connect one end of the power supply to a live AC outlet, then connect the other end to the RASFinder as shown in Figure 2-2. The power connector is a 6-pin circular DIN connector.
5. Turn on power to the RASFinder by setting the ON/OFF switch on the back panel to the ON position.

At this time your RASFinder is completely cabled.

Proceed to the next section to install the RASFinder software.

Adding RAM

A second SIMM connector is provided for adding RAM to the RASFinder. The procedure for adding RAM follows.

1. Ensure that the external power supply is disconnected from the RASFinder.
2. Turn the RASFinder upside down and remove the cabinet mounting screw at the center/back of the cabinet.

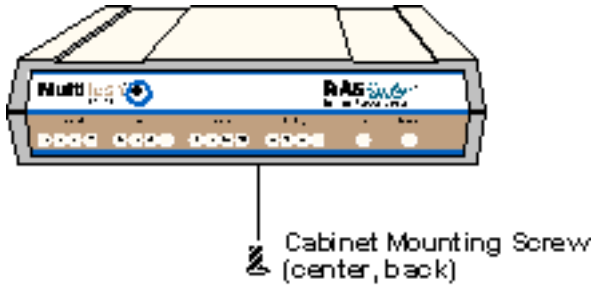


Figure 2-3. Cabinet Mounting Screw

3. Turn the RASFinder right side up, then slide the base out the rear of the cabinet.
4. Position the base so the front panel LEDs are toward you (as in Figure 2-4).

   Note: As long as both SIMMs are identical in type, size, and speed, the RAM in this unit can be expanded from 8 MB to 16 MB, or 32 MB, total.

5. Slant the SIMM at a 45° angle to the back of the base and align the centering notch of the SIMM with the center tab on the SIMM connector.
6. Gently press down on the ends of the SIMM until the two short vertical white pins enter the holes at the ends of the SIMM and the two metal side clips snap in place over the SIMM, locking it down.

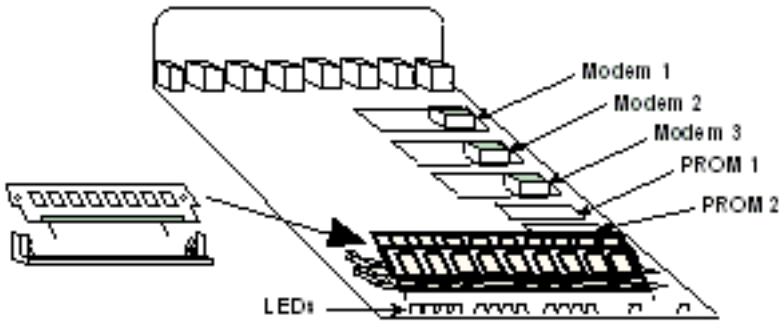


Figure 2-4. Installing a SIMM

7. Align the base with the mating guides on the inside of the cabinet, then slide the base all the way into the cabinet until it stops.
8. Turn the RASFinder upside down and replace the cabinet mounting screw that was removed in step 2.
9. Turn the RASFinder right side up and return to the previous section, Cabling Your RASFinder to connect the cables.

RASFinder™
Remote Access Device

Chapter 3 - Software Loading and Configuration

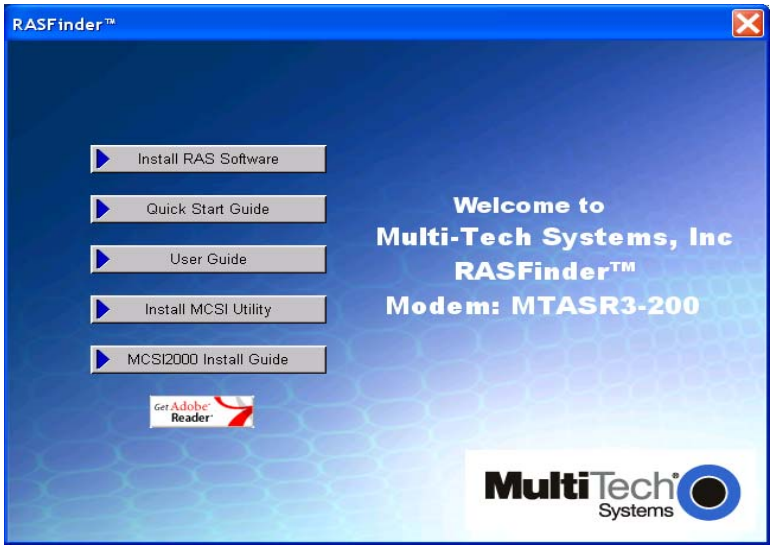
MultiTech® Systems

Installing Your RASFinder Software

The RASFinder software is set up to default to a Remote Access Server (RAS) application. Within the RAS application, you can configure the RASFinder to communicate with a Radius Server for centralized network security or a proprietary Remote User Data base utility to establish your remote user profiles. You can also configure the RASFinder as a router for LAN-to-LAN routing.

The RASFinder CD-ROM contains your RASFinder software, Quick Start and this User Guide. The CD-ROM is auto-detectable and should start automatically when inserted into your CD-ROM drive.

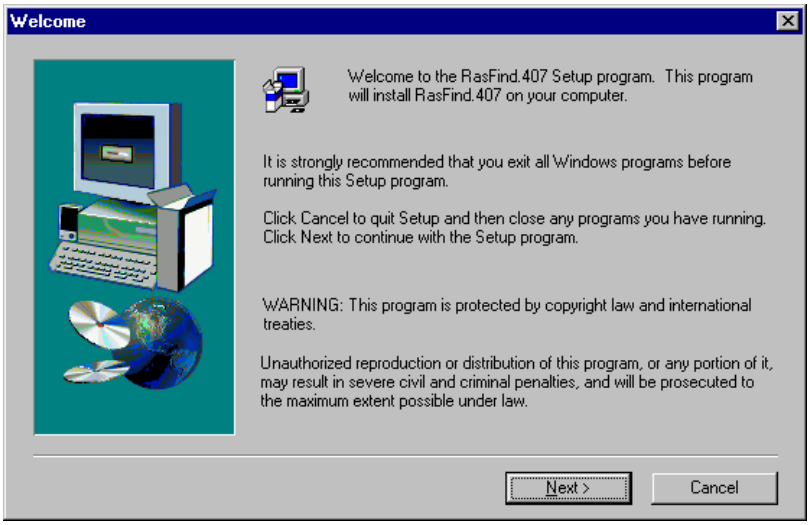
1. Insert the RASFinder CD-ROM into the CD-ROM drive on your local PC. The CD-ROM should start automatically; however, it may take 10 to 20 seconds for the **RASFinder** screen to appear.



If the **RASFinder** Splash screen does not appear automatically, click **My Computer**, right-click the **CD-ROM drive** icon, then click **Autorun**.

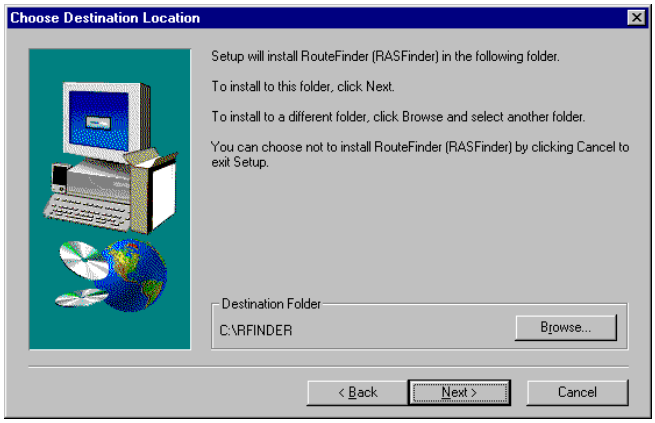
2. When the **RASFinder** screen appears, click the **Install RAS Software** button.

3. The **welcome** screen displays.


Welcome
Welcome to the RasFind.407 Setup program. This program will install RasFind.407 on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Next >
Cancel

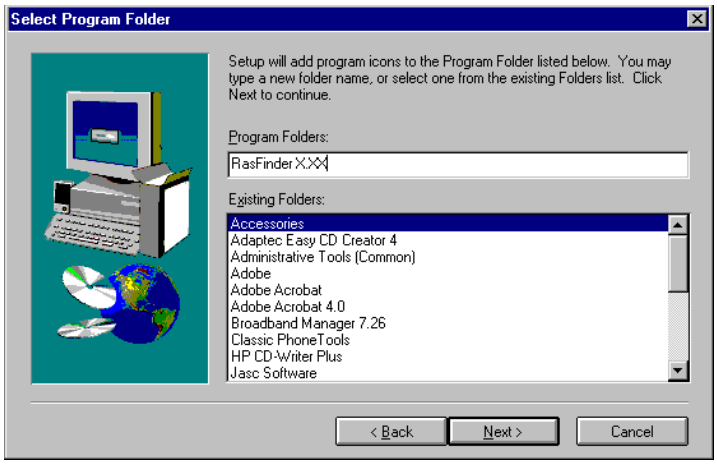
Press **Enter** or click **Next** to continue.

4. The **Choose Destination Location** dialog box displays. Follow the onscreen instructions to install your RASFinder software.


Choose Destination Location
Setup will install RouteFinder (RASFinder) in the following folder.
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
You can choose not to install RouteFinder (RASFinder) by clicking Cancel to exit Setup.
Destination Folder
C:\RFINDER
Browse...
< Back
Next >
Cancel

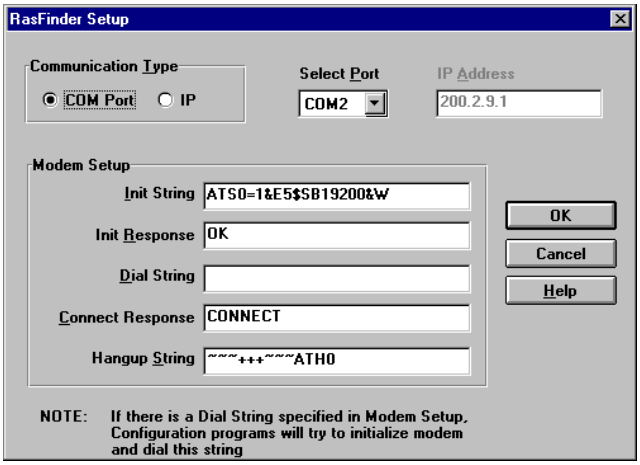
You can either choose a different Destination Location for your RASFinder software by clicking **Browse**, or select the default destination by pressing **Enter** or clicking **Next>.** It is recommended that you accept the default folder, **C:\RASFind.xxx**

5. The **Select Program Folder** dialog box appears.


Select Program Folder
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.
Program Folders:
RasFinder X.XX
Existing Folders:
Accessories
Adaptec Easy CD Creator 4
Administrative Tools (Common)
Adobe
Adobe Acrobat
Adobe Acrobat 4.0
Broadband Manager 7.26
Classic PhoneTools
HP CD-Writer Plus
Jasc Software
< Back
Next >
Cancel

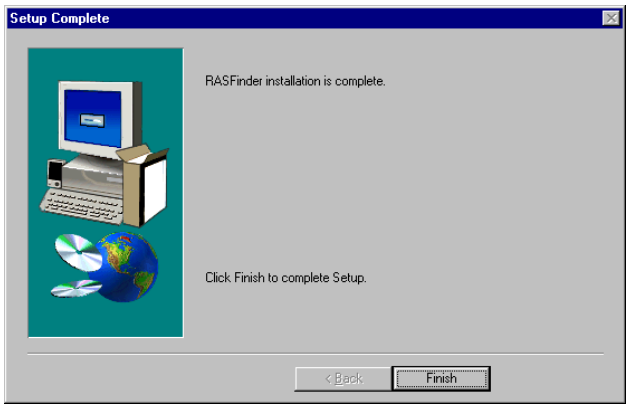
Press **Enter** or click **Next>** to continue

6. The software is loaded onto your PC. The **RASFinder Setup** dialog box is then displayed enabling you to designate the COM port of the PC that is cabled to the RASFinder. From the **Select Port** drop-down box, click the down arrow and select the COM port of your PC (COM1 -- COM4) that is cabled to the RASFinder.



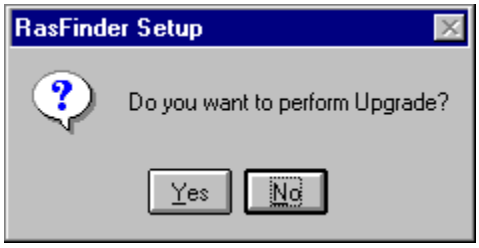
Click **OK** to continue.

7. The **Setup Complete** dialog box displays.



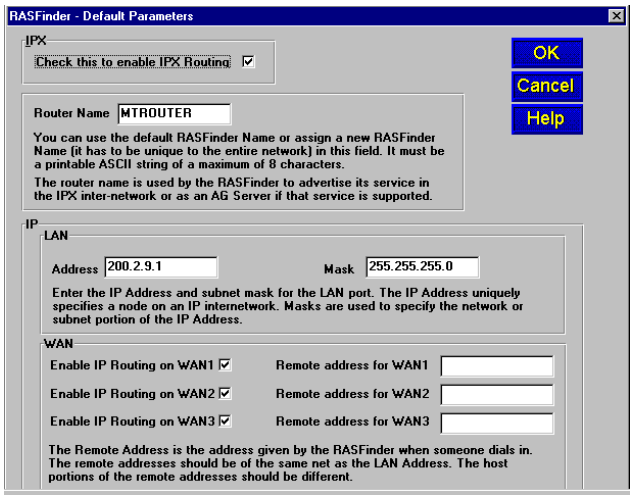
Click **Finish** to continue.

8. The following message displays:



9. Click **No** to skip the upgrade process. The following message appears:

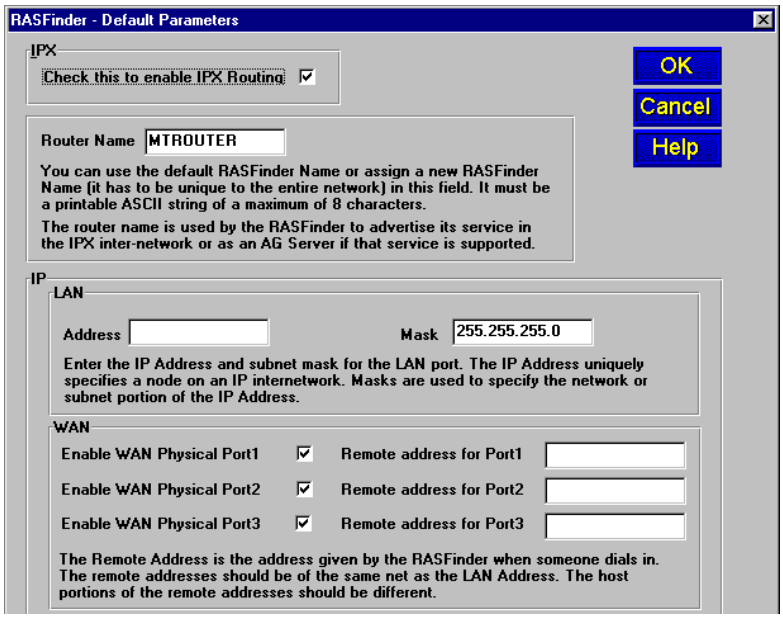
10. Click **Yes** to download the default setup. (Clicking **No** prevents you from setting up the defaults and downloading them to the RASFinder; instead, you are returned to the desktop, where you will see a window with shortcut icons for the various utility programs in the software.)
11. The **Default Parameters** dialog box displays. This dialog box allows you to enable or disable IPX routing, assign the router name (required for IPX routing), establish the IP address and mask for the LAN port, set up remote addresses for the WAN ports, and disable unused WAN ports.


RASFinder - Default Parameters
IPX
Check this to enable IPX Routing
OK
Cancel
Help
Router Name MTROUTER
You can use the default RASFinder Name or assign a new RASFinder Name (it has to be unique to the entire network) in this field. It must be a printable ASCII string of a maximum of 8 characters.
The router name is used by the RASFinder to advertise its service in the IPX inter-network or as an AG Server if that service is supported.
IP
LAN
Address 200.2.9.1
Mask 255.255.255.0
Enter the IP Address and subnet mask for the LAN port. The IP Address uniquely specifies a node on an IP internetwork. Masks are used to specify the network or subnet portion of the IP Address.
WAN
Enable IP Routing on WAN1
Remote address for WAN1
Enable IP Routing on WAN2
Remote address for WAN2
Enable IP Routing on WAN3
Remote address for WAN3
The Remote Address is the address given by the RASFinder when someone dials in. The remote addresses should be of the same net as the LAN Address. The host portions of the remote addresses should be different.

12. If your network protocol is **IPX,** continue with the following step. However, if your network protocol is **IP**, click the **IPX Routing Enable** check box to *disable* IPX, then proceed to step 14.

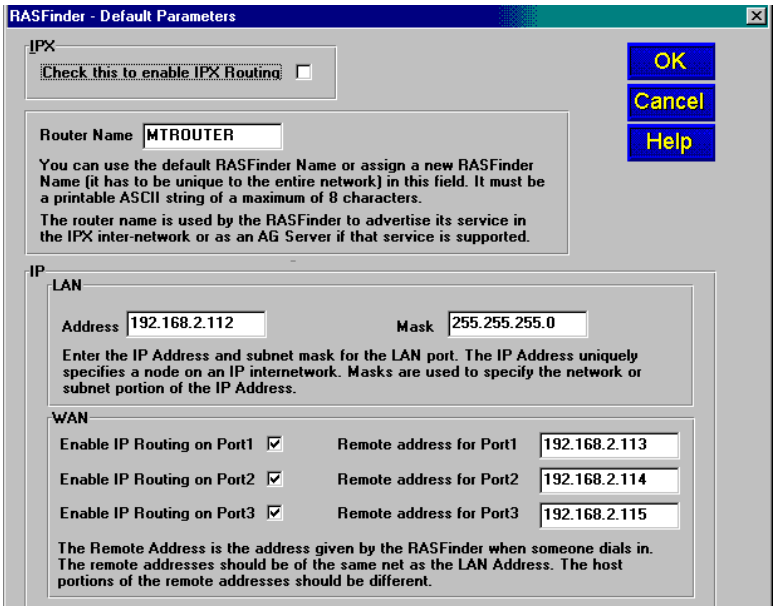
IPX Routing Setup

13. **Router Name:** If this is the only RASFinder on your network, you can use the default Router Name (MTROUTER); otherwise, you must assign a new Router Name in this field. The Router Name can be any printable ASCII string of up to 8 characters (can be mixed uppercase and lowercase). The RASFinder will use this name to advertise its service in the IPX internetwork or as an AG Server, if that service is supported. Proceed to step 15.


RASFinder - Default Parameters
IPX
Check this to enable IPX Routing
OK
Cancel
Help
Router Name MTROUTER
You can use the default RASFinder Name or assign a new RASFinder Name (it has to be unique to the entire network) in this field. It must be a printable ASCII string of a maximum of 8 characters.
The router name is used by the RASFinder to advertise its service in the IPX inter-network or as an AG Server if that service is supported.
IP
LAN
Address
Mask 255.255.255.0
Enter the IP Address and subnet mask for the LAN port. The IP Address uniquely specifies a node on an IP internetwork. Masks are used to specify the network or subnet portion of the IP Address.
WAN
Enable WAN Physical Port1
Remote address for Port1
Enable WAN Physical Port2
Remote address for Port2
Enable WAN Physical Port3
Remote address for Port3
The Remote Address is the address given by the RASFinder when someone dials in. The remote addresses should be of the same net as the LAN Address. The host portions of the remote addresses should be different.

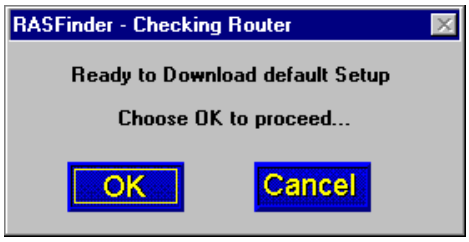
IP Routing Setup

14. For IP Routing, the default Ethernet IP Address has to be changed to your unique LAN address, and the WAN Remote Addresses have to be in the same network as the LAN Address.


RASFinder - Default Parameters
IPX
Check this to enable IPX Routing
OK
Cancel
Help
Router Name MTROUTER
You can use the default RASFinder Name or assign a new RASFinder Name (it has to be unique to the entire network) in this field. It must be a printable ASCII string of a maximum of 8 characters.
The router name is used by the RASFinder to advertise its service in the IPX inter-network or as an AG Server if that service is supported.
IP
LAN
Address 192.168.2.112
Mask 255.255.255.0
Enter the IP Address and subnet mask for the LAN port. The IP Address uniquely specifies a node on an IP internetwork. Masks are used to specify the network or subnet portion of the IP Address.
WAN
Enable IP Routing on Port1
Remote address for Port1 192.168.2.113
Enable IP Routing on Port2
Remote address for Port2 192.168.2.114
Enable IP Routing on Port3
Remote address for Port3 192.168.2.115
The Remote Address is the address given by the RASFinder when someone dials in. The remote addresses should be of the same net as the LAN Address. The host portions of the remote addresses should be different.

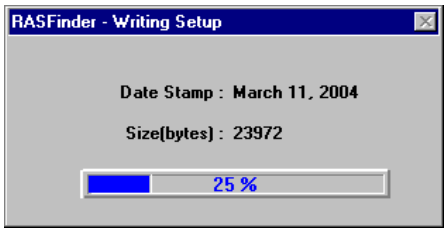
In the IP group, change the default **Ethernet Address** to the value assigned to your RASFinder's LAN port. As you click **OK**, sequential addresses will appear in the Remote address fields for WAN1, 2, and 3. (See above, where the Ethernet IP Address was entered as 192.168.2.112, and the software applied the next three sequential addresses (192.168.2.113,114, and 115) to WAN1, WAN2, and WAN3, respectively.)

15. The following message displays.

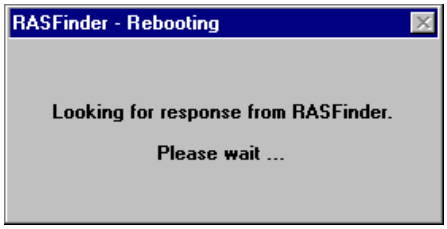


Click **OK** to proceed.

16. The **Writing Setup** dialog box (with the current date and the file size in bytes) displays as the setup configuration is written to the RASFinder.



17. Next, the **Rebooting** dialog box displays.



18. Check to ensure that the **Fail** LED on the RASFinder goes Off after the download is complete and the RASFinder is rebooted (the **Rebooting** dialog box goes away). This may take several minutes as the RASFinder reboots.

19. If you are going to establish your remote user profile database using the proprietary Remote User Database utility, proceed to the next section, or if you are going to use a Radius server for centralized network security, proceed to the section entitled, Setting Up Remote Access Dial In User Server (RADIUS).

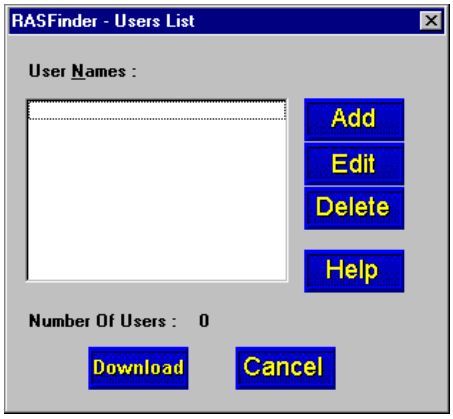
    For Routing, proceed to the last section (Final Routing Setup) in this chapter to set up the RASFinder as a router.

Setting Up Your Remote User Database

The propreitary Remote User Data Base supports remote dial-in users for user name, password, and port availability. Each dial-in user needs an entry in this database. You can add remote users, remove users, or edit information in the database.

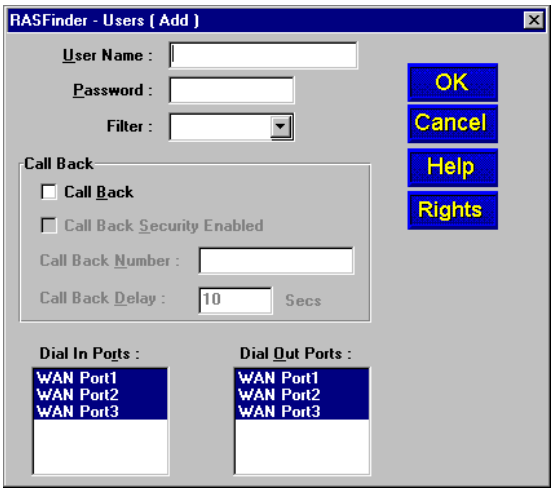
1. From your desktop, click **Start | Programs | RASFinder x.xx | Remote User Data Base,** or double-click the **Remote User Data Base** icon in the **RASFinder x.xx** icon group window (below).

2. An **Accounting Info - Read** screen appears briefly, then the **Users List** dialog box displays.



Click **Add**.

3. The **Add Users** dialog box displays.



4. Build your user database by filling in the following fields for each user.

User Name

The User Name can have as many as 39 characters. All printable characters are permitted with the restriction that no blanks are allowed in the user name. In dial-in and dial-out applications, the user name is treated as a case insensitive string.

User Password

The User Password can have as many as 7 characters. In places where the password is used as a character string, it is treated as a case insensitive string. Elsewhere (PPPs CHAP), it is treated as a case sensitive pattern.

Filter

The drop-down list enables you to select the unique filter entry that was defined in the ID field in the **Add/Edit Filters** dialog box. This filter ID must be a unique alphanumeric identifier of up to 9 characters in length that identifies the remote user.

Call Back

You have to click this check box to enable the Call Back function. If the user is at a location where he wants to be called at then he must be allowed to choose the specific location where he wants to be called back at. To do this, the Call Back option must be enabled (activated) and the Call Back Security Enabled option must NOT be enabled (activated). The remote user would then use a standard PPP client or ASCII terminal dial-in.

To enable Call Back Security, the Call Back option must be checked (activated) and the following three boxes/fields filled in.

- **Call Back Security Enabled**

  This parameter is of use in dial-in applications where the user must always be called back at a specific location. Enabling this parameter (Alt-S) results in having the administrator assigning the call back parameters. Leave this function disabled if the user is to be allowed to choose the call back number and the call back delay.

- **Call Back Number**

  The Call Back Number is editable only if Call Back Security is enabled (checked). This is the number where the user will be called back. The user **cannot** choose the location where he wants to be called back.

  Note: You can enter the Call Back Number with or without dashes, the modem will simply ignore them.

- **Call Back Delay**

  Call Back Delay is editable only if Call Back Security is enabled. This specifies the duration (in seconds) after which the user will be called back at the administrator-assigned number.

Dial In Ports

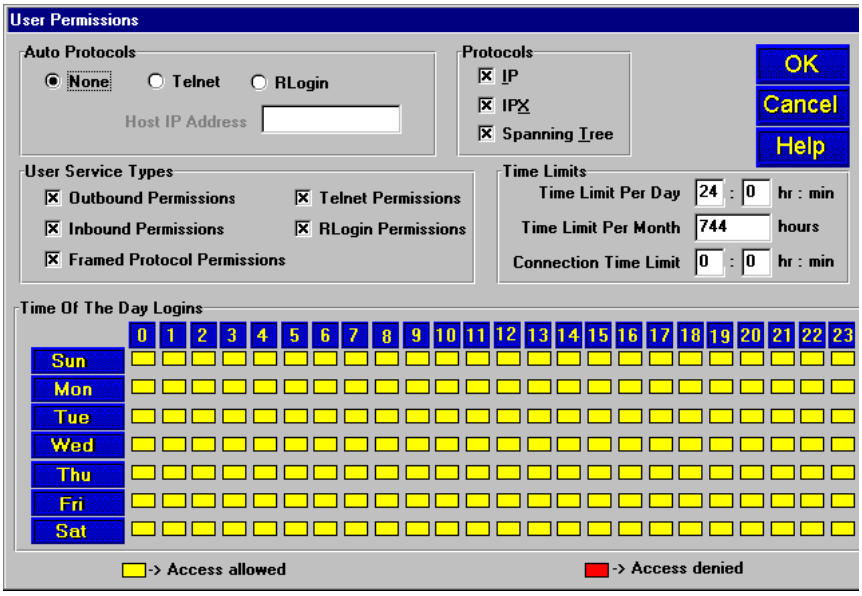
The systems administrator can enable (highlight) WAN Ports 1, 2, and/or 3 to be made available for dialing in to the RASFinder.

Dial Out Ports

The systems administrator can enable (highlight) WAN Ports 1, 2, and/or 3 to be made available for dialing out from the RASFinder.

Click the **Rights** button to assign user permissions for the remote user.

5. The **User Permissions** dialog box displays.



6. Build your user permissions by filling in the following fields for each remote user.

Auto Protocols

This group enables the systems administrator to assign unrestricted LAN/Intranet access or limited protocol access. You have the following three options.

- **None**

  This option allows the user to have unrestricted access to the LAN/Intranet. This is the default setting.

- **Telnet**

  This option allows Telnet sessions between the designated server (defined by the Host IP Address field) and the remote users. Telnet is an applications-level protocol commonly found in IP-based networks that allow terminal emulation at a remote workstation. If you select Telnet, you are required to enter an IP address in the Host IP Address field. This limits the user to only specific functions on the network.

- **RLogin**

  This option allows the RASFinder to be used as an RLogin client for connecting to an RLogin Server (defined by the Host IP Address field). RLogin is an application protocol that provides a terminal interface between Unix hosts using TCP/IP network protocol. Unlike Telnet, RLogin assumes that the remote host is a Unix machine. If you select RLogin, you are required to enter an IP address in the Host IP Address field. This limits the user to only specific functions on the network.

Host IP Address

Enter the IP Address for the Telnet or RLogin host computer (server). The Host IP Address must be in dotted-decimal notation format.

Note: This field is only enabled (activated) when either Telnet or RLogin have been enabled.

Protocols

The Protocols group enables you to limit the remote user to IP routing, IPX routing, or bridging (Spanning Tree); or, a combination of any two or all three routing protocols. The default setting enables all three protocols.

User Service Types

The User Service Types group enables you to set the permissions for the entry being configured. The systems administrator can enable or disable the following options to customize the types of services for a particular remote user. By default, all permissions are enabled. To deny permissions to the entry being configured, click (check) the box to the left of the permission to disable the feature.

- **Outbound Permissions** - grants the remote user dial-out rights.
- **Inbound Permissions** - grants the remote user dial-in rights.
- **Framed Protocol Permissions** - grants the remote user framed protocol rights (e.g., Framed Protocol – PPP). By enabling (checking) this option, the user becomes an unrestricted user (i.e., both framed and unframed protocols are allowed).
- **Telnet Permissions** - grants the remote user Telnet file transfer rights.
- **RLogin Permissions** - grants the remote user RLogin server connection rights.

Time Limits

The Time Limits group enables the systems administrator to impose time-related restrictions to the entry being defined.

Note: The **SNTP Client** check box must be selected in the **SNTP Setup** dialog box and pointed to a valid time protocol server in order to monitor Time Limits and Time of the Day Logins.

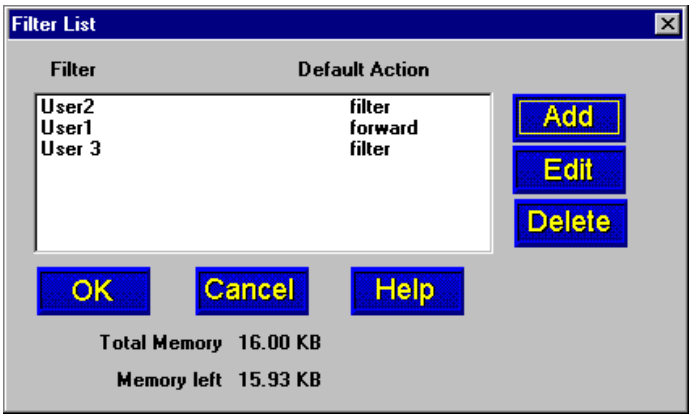
Time of the Day Logins

The User Permission grid enables the administrator to deny a remote user Internet access at certain times during the week. This would be applicable when the administrator wants to bring a system down for a particular reason and does not want users to access the Internet at that time.

By default, all time periods are color-filled with yellow indicating that the remote user has permission to access the Internet all the time. To deny permission for certain periods of time, click all applicable yellow boxes over the target time range to toggle them to red (Access Denied).

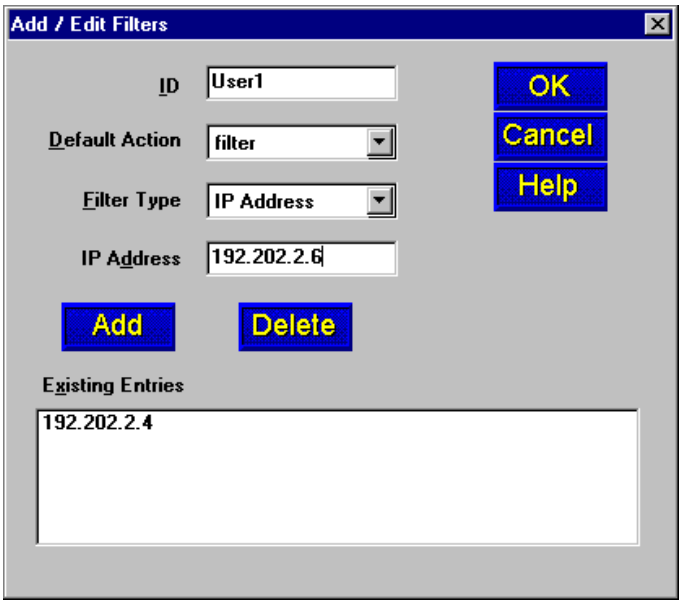
7. After each user is defined in the **Add Users** dialog box and the user permissions (Rights) have been configured, click **OK** to display the updated **Users List** dialog box. Click **Filters** to add filtering parameters for the remote user entry.

8. The **Filters List** dialog box displays.



Click **Add**.

9. The **Add/Edit Filters** dialog box displays.



10. Build your filtering parameters by filling in the following fields for each remote user.

    ID

    This field requires a unique ID identifying the remote user. The ID can be the name of a person, a work station, or a remote user identified simply as “User 1”. The ID can be up to 9 alphanumeric characters in length.

    Default Action

    This drop-down list enables you to select either **filter** or **forward**. If you select filter, then the entry will be transmitted with filtering properties. If you select forward, then the entry will be transmitted without filtering properties. The default setting is filter.

    Filter Type

    The Filter Type drop-down list enables you to select the filter type. The filter types are either IP Address, Protocol, or Domain Name. The default setting for Filter Type is IP Address.

    - **IP Address** – If the filter type is IP Address, enter the IP Address of the remote user in dotted-decimal notation format.
    - **Protocol** – If you select Protocol as the filter type, the **Add/Edit Filters** dialog box is displayed with Protocol and Port drop-down list fields. Select either TCP or UDP from the Protocol drop-down list and select either Telnet, FTP, or SFTP from the Port drop-down list.
    - **Domain Name** – If you select Domain Name as the filter type, the **Add/Edit Filters** dialog box displays with a Domain Name field. Eenter the domain name consisting of a sequence of names separated by periods (dots) followed by an extension, e.g., “pictures. computers.com.” The domain name can be up to 39 alphanumeric characters including periods.

    Note: Current filter entries are displayed in the Exisiting Entries window.

    Click **OK** to add the remote user to the **Filters List** dialog box and then click **OK** again to return to the **Users List** dialog box.

11. Click **Add User** to continue adding users to your database.

12. When you have added all users to the database, click **Download** to write the database to the RASFinder.

Setting Up Remote Access Dial In User Server (RADIUS)

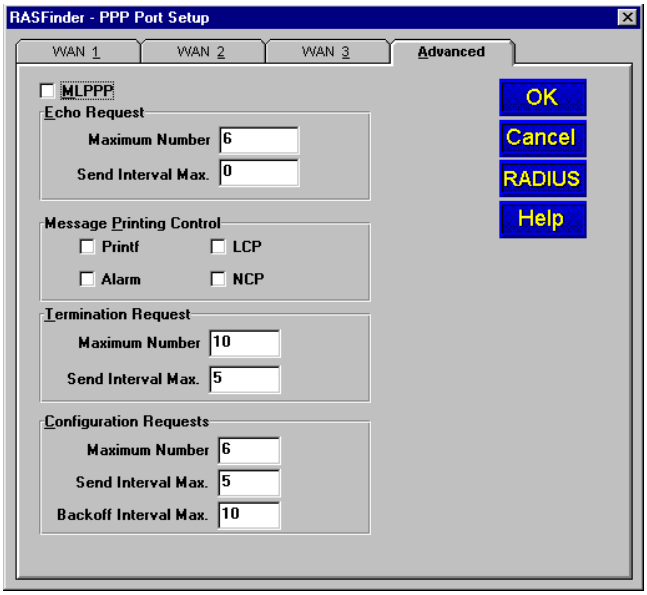
RADIUS is an optional security feature that uses a single authentication server to centralize security on networks with large modem pools, especially those with multiple communication servers.

1. From your desktop, click **Start | Programs | RASFinder x.xx | RASFinder Configuration**, or double-click the **RASFinder Configuration** icon in the **RASFinder x.xx** icon group window when it displays on your desktop.

2. The main menu (**Router Setup**) displays.

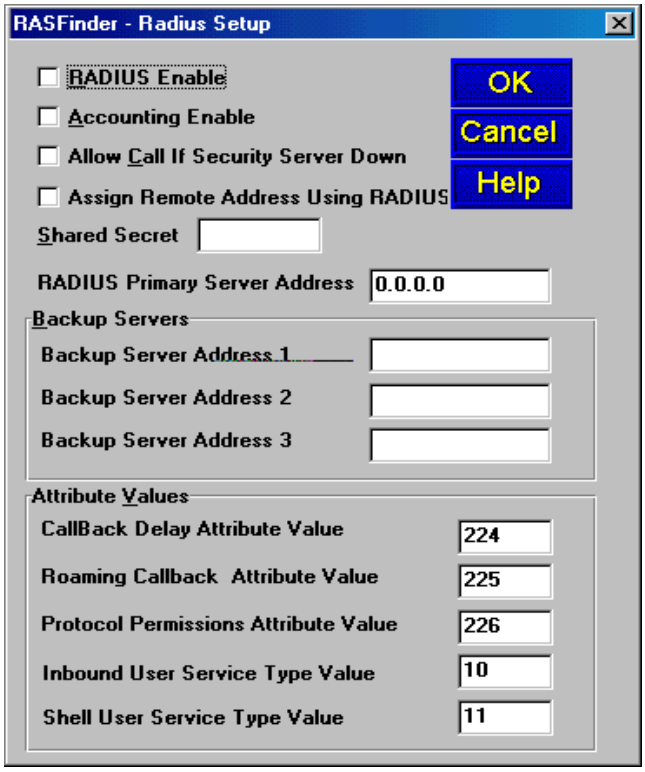
Click **PPP / SLIP** to continue.

3. The **PPP Port Setup** dialog box displays; click the **Advanced** tab.



Click **RADIUS** to continue.

4. The **Radius Setup** dialog box displays.



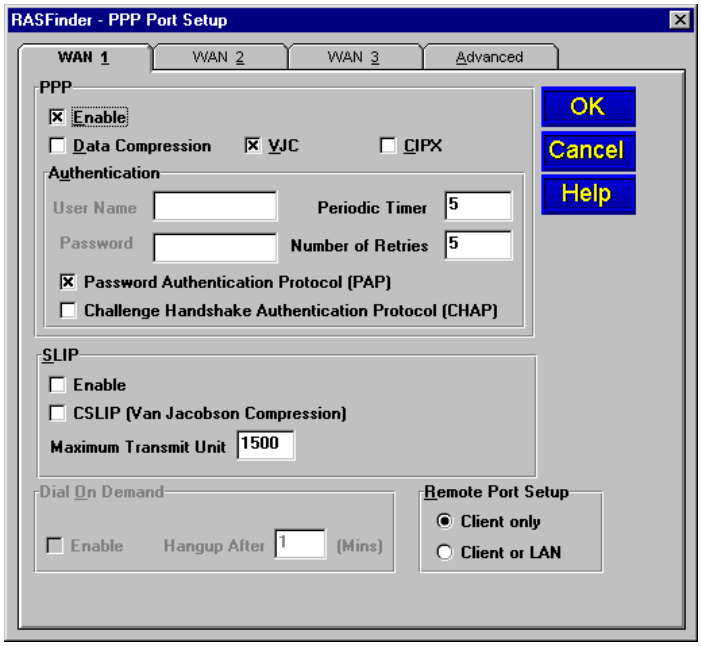
5. Click **RADIUS Enable** to enable Radius security services for all ports on this RASFinder.
6. Click **Accounting Enable** if you want Radius to track accounting information such as login and logout times, bytes sent and received, etc.
7. Leave **Allow Call if Security Server Down** unchecked (disabled) to prevent users from logging in if the security servers are down.
8. Click **Assign Remote Address Using RADIUS** to enable the Radius Server to automatically assign the IP Address of the WAN port on the RASFinder that the user will dial into.
9. Obtain the **Shared Secret** from the Radius network administrator. The Shared Secret must be the same secret that is used on the Radius server whose address is being supplied for the Radius primary server address entry.
10. Obtain the Radius server address from the Radius network administrator that will provide the security to the RASFinder. The Radius server address is to be enterred in the **RADIUS Primary Server Address** field.
11. If additional servers are being used as backup servers, obtain their address(es) from the Radius network administrator and enter them in Backup Servers group. The first backup server address is enterred in the **Backup Server Address 1** field. Any additional backup server addresses are to be enterred in the **Backup Server Address 2** and **Backup Server Address 3** fields.
12. A set of default attribute values will be displayed in the **Attribute Values** group. These default values are used with the Multi-Tech Radius Server. You do **not** have to change these values if your RASFinder is communicating with Multi-Tech's Radius Server. If you are using another vendor's Radius Server to communicate with your RASFinder, you will have to communicate with your Radius Server network administrator to see how he/she has set up these attribute values and then change the default values to the values being used by that Radius server.

Final Routing Setup

1. From your desktop, click **Start | Programs | RASFinder x.xx | RASFinder Configuration**, or double-click the **RASFinder Configuration** icon in the **RASFinder x.xx** icon group window when it displays on your desktop.
2. The main menu (**Router Setup**) displays.

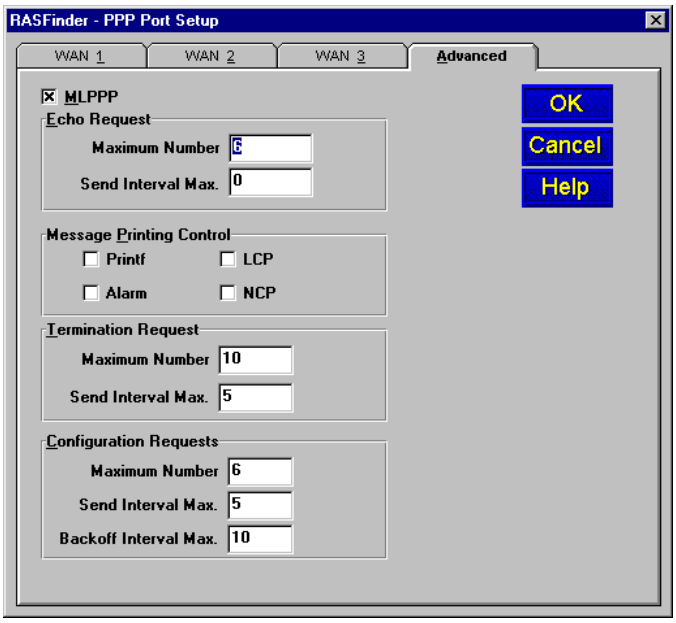
Click **PPP/SLIP** button to continue.

3. The **PPP Port Setup** dialog box displays.



On the **WAN 1** tab, click **Client or LAN** in the **Remote Port Setup** group in the bottom right corner; this enables **Client or LAN** and disables the default, **Client only**. Repeat this on the **WAN 2** and **WAN 3** tabs in turn.

4. If you are going to combine the three WAN ports together, i.e., a single IP address, you need to enable the **MLPPP** option from the **Advanced** tab.

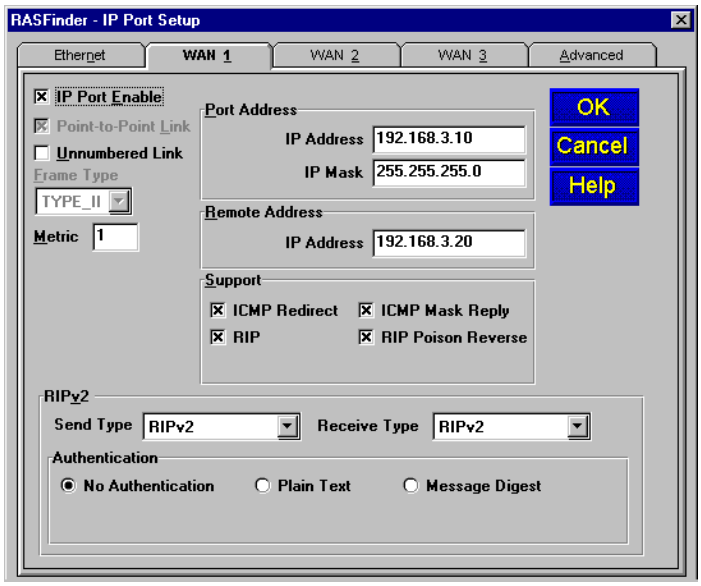


Note: When the dialog box "When a PPP port is Client-or-LAN type:" appears, click on the OK button each time the dialog box appears. You are returned to the Main menu.

5. From the Main menu, click on the **IP** button and the **IP Port Setup** dialog box appears with the Ethernet tab active and the Port Address displaying your LAN IP Address.

Click on the **WAN 1** tab

6. On the WAN 1 tab, change the **Port Address** and **Remote Address** groups to be on separate networks from the Ethernet LAN port.



If you enabled MLPPP option on the PPP Port Setup dialog box, the IP addresses for all three WAN ports have to be identical and the remote WAN port addresses have to be within the same network and identical.

If you did not enable MLPPP option, the WAN port addresses have to be on a different network from the LAN port address and have to be different from each other.

7. Click on each of the WAN tabs and change the **Port Address** group and **Remote Address** group to conform with the settings for WAN 1.

8. Click **OK** to return to the Main menu.

9. From the Main menu, click **Download Setup** button to write your new configuration to the RASFinder. After your configuration is written to the RASFinder, you are returned to the Main menu. Your RASFinder is now configured for LAN-to-LAN routing.

RASFinder™
Remote Access Device

Chapter 4 - RASFinder Software

MultiTech® Systems

Introduction

This chapter describes the RASFinder software and explains how to make changes to the configuration of your RASFinder. The major configuration parameters were established during the loading of the software (Chapter 3) and initial configuration. The RASFinder software and configuration utilities enable you to make changes to that initial configuration.

The RASFinder software enables you to refine your configuration based on your network connections. The software is based on a main menu (RASFinder - Router Setup) that enables you to consider all the parameters for a particular feature (e.g., IP or IPX protocol, Bridging, or setting up a WAN port for PPP or SLIP protocol). These features, and others are discussed in detail in the RASFinder Configuration section later in this chapter.

There are eight configuration utilities that offer additional functionality. The **RASFinder Configuration** utility brings up the main menu (RASFinder - Router Setup) screen that provides you with access to the buttons that enable you to view or change your initial configuration. The **Download Firmware** utility enables you to download new versions of firmware when enhancements become available. The **Download Default Setup** utility enables you to specify a set of parameters that are unique to your unit. The **Configuration Port Setup** utility enables you to change the direct connection of a PC to the Command Port on the RASFinder. The **Uninstall *RASFinder* Configuration** utility is designed to remove the software from your PC. The **Upgrade RASFinder** utility will check to see if your RASFinder is using the latest software version and then, if necessary, guide you through the upgrade process. The **WAN Device Configuration** utility opens the Print Console, a terminal emulation program that enables you to configure the built-in modems. The **Remote User Data Base** utility (supported through the command port) enables you to establish and maintain a database of information about your remote users. You can add and remove remote users, or edit existing user information in the database.

Your RASFinder software includes a context-sensitive Help system. Clicking the Help button on any given dialog box provides definitions and recommended values for each button, option, and field on that dialog box. In some instances, you will also see a list of related topics that can be displayed by clicking green, underlined text. In addition, you can use the Index tab to search the entire Help system for definitions and references to specific terms, fields, and recommend values where applicable.

Before You Begin

The RASFinder software operates in a Microsoft Windows® environment. Your **RASFinder x.xx** program group, with all the utilities described above, is accessible by clicking **Start | Programs | RASFinder x.xx | *(utility)***, or by double-clicking the utility icon in the program group in **My Computer** (**C:\Windows\Start Menu\Programs\RASFinder x.xx** in Windows 98). The program group is shown here:

RASFinder Setup

All changes to your RASFinder configuration are initiated through the RASFinder - Router Setup menu. You can view or change your RASFinder configuration in Windows 98, 2000, XP and Windows NT by clicking **Start | Programs | RASFinder | Router Configuration**, or double-clicking the Router Configuration icon in the RASFinder program group, if it displays on your desktop. After loading, the **RASFinder - Router Setup** menu displays.

The **RASFinder - Router Setup** menu consists of 13 buttons that enable you to display and change your protocols, define the output of the RASFinder, perform network management functions, test the communications link, print messages received from the target RASFinder, and download setup information to the RASFinder.

The two outer buttons in the bottom row are used to open the on-line Help system (RASFinder Setup Help) and end (Exit) a Router Setup session. The middle (Retry) button remains inactive unless you fail to connect to the target RASFinder.

Typical Applications

The two basic applications for the MTASR3-200 RASFinder are (1) as a Remote Access Server (RAS) to permit remote users to dial into a local area network and use the resources of that network and (2) as a Router for LAN-to-LAN routing. The RASFinder defaults to a RAS configuration during the initial software loading. Typical examples of both types of applications are presented in the following paragraphs.

RAS Applications

During the initial software installation, the RASFinder defaults to a remote access server (RAS) configuration. For example, the WAN Ports are connected to individual phone lines and the ports are then configured to answer incoming calls from remote locations. Two methods of identifying remote users are provided in the RASFinder; 1) Remote Access Dial In User Server (RADIUS) and 2) a Remote User Data Base utility in the RASFinder software.

RAS Application Using Radius

RADIUS is associated with a Radius server on the network which provides a security feature using a single authentication server to centralize security on a network. The Remote User Data Base utility identifies each user by user name, password and, if Call Back Security is enabled, a specific phone number the RASFinder must call to establish the connection with the remote user.

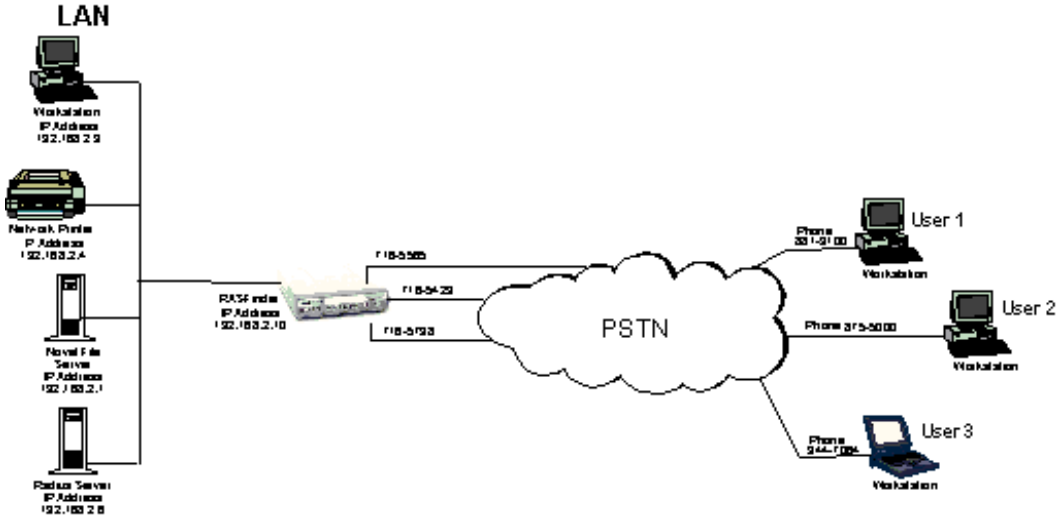


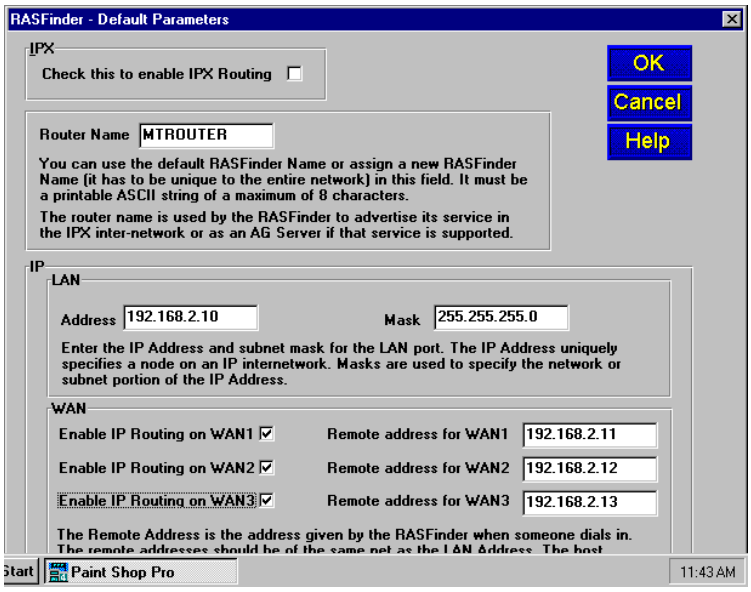
Figure 4-1. RAS Application

Before remote users can dial into the network, either the Radius security services have to be established, or each remote user must be idenfitied in the Remote User Data Base. Radius provides a single secure server for all remote users; whereas the Remote User Data Base utility identifies each user by User Name, Password, and a specific Call Back Number if Call Back Security is enabled. Radius and the Remote User Data Base have to have communication between the remote user and the administrator either for setting up the data base or the security services to establish a user profile. Radius also requires communication between the Radius administrator and the RASFinder administrator to set up the security features and the Radius server address.

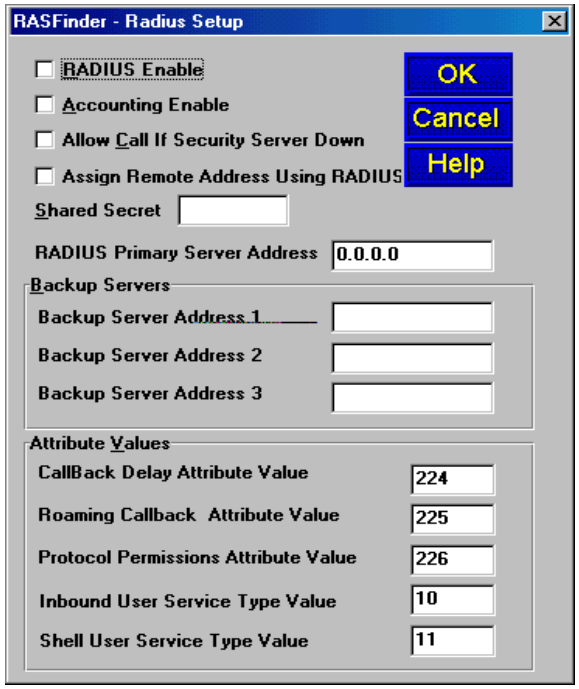
For a typical RAS application with a Radius server providing the network security, the Ethernet (10Base-T or 10Base-2) port of the RASFinder is connected to the IP network, the Radius server is on the backbone of the network, and the WAN ports of the RASFinder are connected to individual phone lines. During initial software installation, the **Default Parameters** dialog box displays with both IPX and IP protocols enabled and a default Ethernet IP address and (subnet) mask displayed. For a RAS application using Radius on an Ethernet IP network, you would disable the IPX protocol and then change the default LAN IP address and mask to the unique IP addressing scheme for your

network. The address assigned to the Ethernet port of the RASFinder can be any address that is recognizable by your network's backbone.

After you enter your LAN IP address information and three sequential WAN addresses have been automatically placed in the Remote address for WAN 1, 2, and 3 fields, ensure that the Enable IP Routing on WAN 1, 2, and 3 are checked. This activates the WAN ports to receive calls from the remote users. At this point, the software will be downloaded to the RASFinder and then you will need to go in through the main menu and set up the conditions for the Radius security services.


RASFinder - Default Parameters
IPX
Check this to enable IPX Routing
OK
Cancel
Help
Router Name MTROUTER
You can use the default RASFinder Name or assign a new RASFinder Name (it has to be unique to the entire network) in this field. It must be a printable ASCII string of a maximum of 8 characters.
The router name is used by the RASFinder to advertise its service in the IPX inter-network or as an AG Server if that service is supported.
IP
LAN
Address 192.168.2.10
Mask 255.255.255.0
Enter the IP Address and subnet mask for the LAN port. The IP Address uniquely specifies a node on an IP internetwork. Masks are used to specify the network or subnet portion of the IP Address.
WAN
Enable IP Routing on WAN1
Remote address for WAN1 192.168.2.11
Enable IP Routing on WAN2
Remote address for WAN2 192.168.2.12
Enable IP Routing on WAN3
Remote address for WAN3 192.168.2.13
The Remote Address is the address given by the RASFinder when someone dials in.
Start
Paint Shop Pro
11:43 AM

To enable the Radius security services, you need to establish communications between the Radius server and the RASFinder. The Radius security service options are defined on the **Radius Setup** dialog box. To provide vendor-specific configuration for the Radius server, you need to bring up the main menu, hit the PPP/SLIP button, and click the RADIUS button in the **PPP Port Setup** dialog box.



The **Radius Setup** dialog box enables the RADIUS option, establishes accounting, enables call if security server is down, assigns a remote address using the RADIUS, provides a window for the shared secret, and indicates the primary RADIUS server IP address. The new vendor specific attributes and services that you establish for the RASFinder can not conflict with any standard Radius

attributes or any other custom attributes on the Radius Security Server. The Enable RADIUS option enables communication between the Radius server and the RASFinder. Enable Accounting option activates the accounting features which allow the Radius server to track the number of bytes sent and received, login and logout times, port number, etc. The Allow Call If Security Server Down feature can be used when the Remote User Data Base Utility is used as a backup database to the Radius security services. The Assign Remote Address Using RADIUS feature enables the Radius server to take over the addressing scheme of the WAN ports on the RASFinder.

The Shared Secret is an entry that must be obtained from the Radius network administrator and must be the same as is used on the Radius security server. The RADIUS Primary Server Address is the IP address of the Radius security server and in our typical RAS application, this address is 192.168.2.6. If one or more backup Radius servers are used in your network, then their IP addresses need to be entered in the Backup Server Address 1, 2, and/or 3 fields.

The Attribute Values Group at the bottom of the **Radius Setup** dialog box needs to have the value for each of the three attributes and two services filled in.

The three new attributes are vendor-specific attributes and may have to be added to the Radius server dictionary. The first attribute is Callback-Delay with a value of 224. The Radius server is set up with a delay time for calling back the remote user. The Roaming-Callback attribute has a value of 225. This attribute specifies a telephone number of where a remote user can be called back if he/she is not at their usual telephone number provided in their user profile. The remote user would have to give that new phone number to the Radius network administrator so the RASFinder will know that the remote user is at a different phone from the one in their user profile.

The Protocol Permissions Attribute has a value of 226 and the values associated with the attribute are “1” for IP, “2” for IPX, and “3” for Spanning Tree.

The Inbound User Service Type Attribute has a value of “10” and an associated value of “6”. This attribute enables the remote user to have inbound access to the network only; in other words, this attribute *adds* inbound access to the remote user’s profile.

The Shell User Service Type Attribute has a value of “11” and also an associated value of ”6”.

After these new attributes are added to the Radius server and the user profile is established, a remote user (in our typical RAS application with Radius, Remote User 1, for example) could call into the RASFinder and identify themselves by their user name and password. Remote User 1, in our typical application, can initiate a dialup session by entering their User name and password in the Dial-Up Networking (My Connection) dialog box and the phone number of the WAN port on the RASFinder that User 1 is going to be connected to. In this application, remote user 1 could dial 716-5565 to connect to WAN port number one on the RASFinder.

At this point, Remote User 1 has access to the services on the LAN. For instance, if he/she wanted to print a report, it could be sent to the printer and printed out as if Remote User 1 was on the local area network.

RAS Application using Remote User Database

The initial software loading process would be the same as for the RAS application using Radius, except that now instead of setting up Radius parameters, you will assemble a Remote User Database. A typical RAS application using the Remote User Database is shown in Figure 4-2.

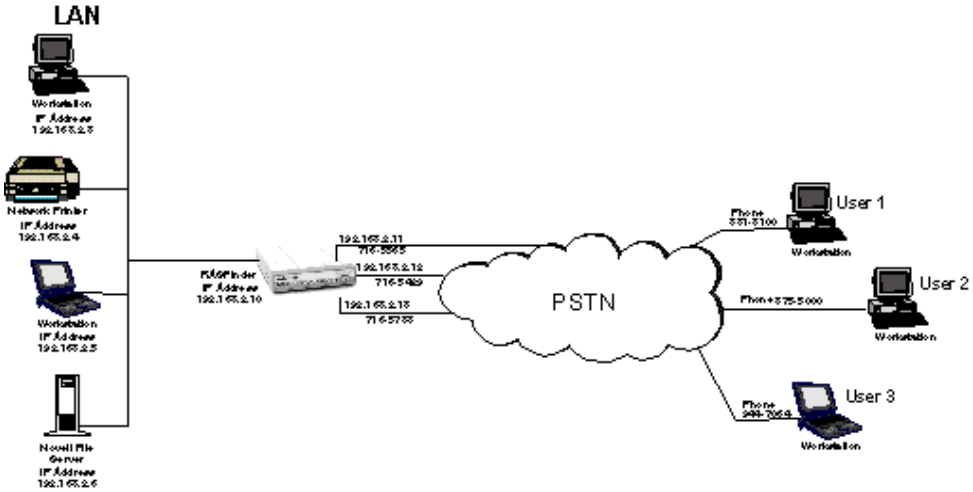
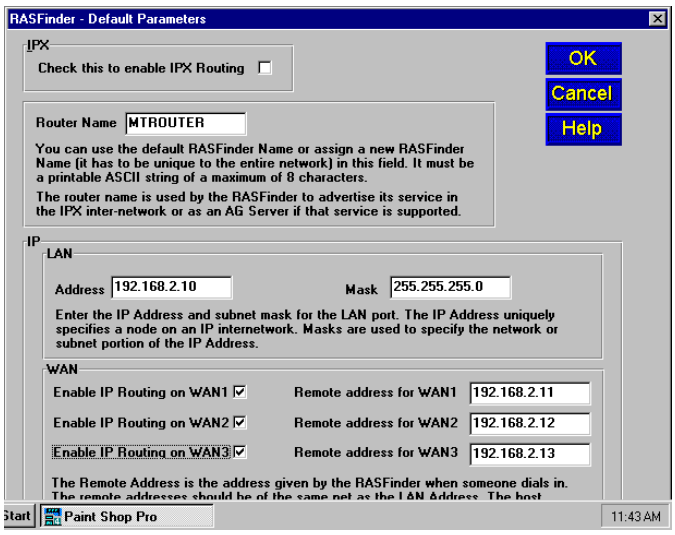


Figure 4-2. RAS Application using Remote User Data Base

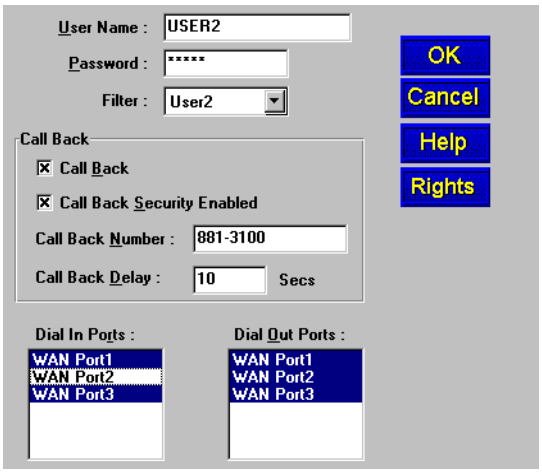
During the software loading process when the **Default Parameters** dialog box displays, both IPX and IP protocols are enabled and a default Ethernet IP address and (subnet) mask are displayed in the IP LAN group. For this RAS application, you would disable the IPX protocol and then change the default LAN IP address and mask to the unique IP addressing scheme for your network. The address assigned to your RASFinder's Ethernet port can be any address that is recognizable by your network's backbone.

In this typical RAS application, the IP network address is 192.168.2.xxx. For the purpose of this discussion, we are assigning the IP address 192.168.2.10 to the Ethernet port on the RASFinder. After this address is entered into the IP Address field of the Default Parameters dialog box, the next three sequential IP addresses (192.168.2.11, 192.168.2.12, and 192.168.2.13) are assigned to the WAN ports. These three IP addresses, in the same network (with the Ethernet LAN), are associated with the respective WAN ports so that when the remote users dial into the WAN ports, they *always* appear (to the rest of the IP network) at these respective addresses.


RASFinder - Default Parameters
IPX
Check this to enable IPX Routing
OK
Cancel
Help
Router Name MTROUTER
You can use the default RASFinder Name or assign a new RASFinder Name (it has to be unique to the entire network) in this field. It must be a printable ASCII string of a maximum of 8 characters.
The router name is used by the RASFinder to advertise its service in the IPX inter-network or as an AG Server if that service is supported.
IP
LAN
Address 192.168.2.10
Mask 255.255.255.0
Enter the IP Address and subnet mask for the LAN port. The IP Address uniquely specifies a node on an IP internetwork. Masks are used to specify the network or subnet portion of the IP Address.
WAN
Enable IP Routing on WAN1
Remote address for WAN1 192.168.2.11
Enable IP Routing on WAN2
Remote address for WAN2 192.168.2.12
Enable IP Routing on WAN3
Remote address for WAN3 192.168.2.13
The Remote Address is the address given by the RASFinder when someone dials in.
Start
Paint Shop Pro
11:43 AM

Before remote users can dial into the network, a user profile has to be set up in the proprietary remote user database using the Remote User Data base utility. This data base utility is provided with the RASFinder software. The RASFinder network administrator builds this database by adding

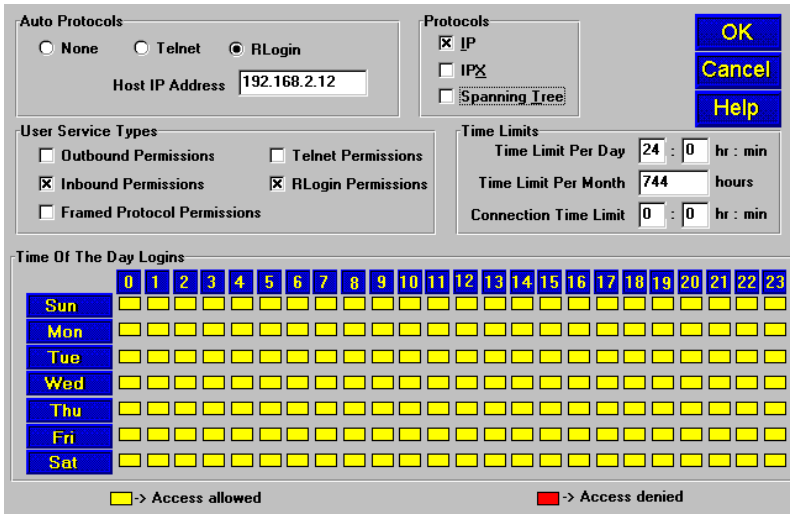
information (for one remote user at a time) via the Add Users dialog box. The user name and password in this application must be negotiated between the RASFinder administrator and each remote user.



User names can be up to 39 characters long, with any printable characters; however, no spaces are allowed within the names. In our dialog box (above), we are using the User Name “User2.” The letters will appear as all caps in the Users List; however, dial-in applications will treat the user names as case-insensitive strings, enabling the users to enter their user names as all uppercase, all lowercase, or a mixture of uppercase and lowercase.

A User Password of up to 7 characters should be given each user. In the Call Back group, the **Call Back** option should be enabled (checked) for security purposes. If ONLY this option is checked, the remote user would be asked to supply the callback numbers when they dial into the RASFinder. If **Call Back Security Enabled** is also checked, the administrator controls the callback numbers through the **Call Back Number** field. In our typical application, User 2’s phone number is 875-5000; therefore, we enter this number in the Call Back Number field. In the Dial In Ports, we have assigned User2 to WAN Port 2 with phone number 716-5429 assigned to it. This phone number will have to be entered in the Phone Number field on remote User 2’s dial-up networking (My Connection) dialog box.

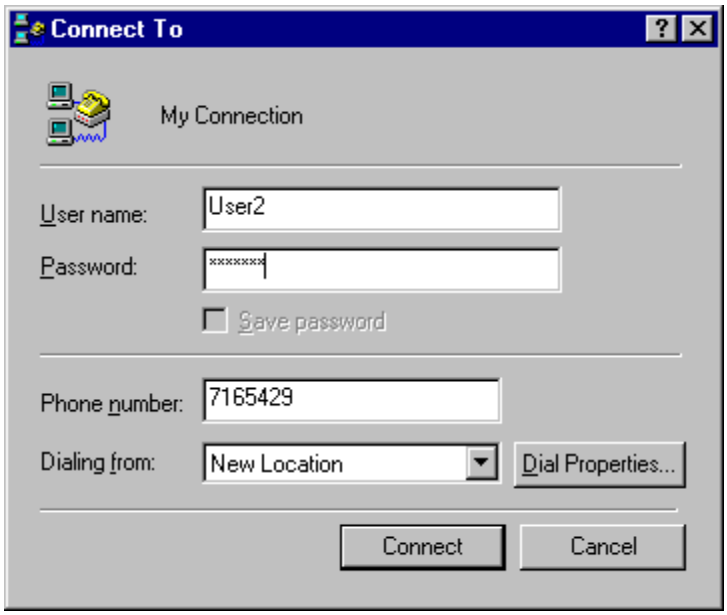
After the Add Users dialog box is filled in, you need to click the Rights button which brings up the **User Permissions** dialog box.



The **User Permissions** dialog box enables you to assign protocol’s, user service type(s), time limits, and time of day for each user to login. The Auto Protocols allow for no auto login, login via Telnet, or RLogin and then direct the remote user to a specific host. The User Service Types defines how the remote user is going to be allowed to use the network. For example, a remote user could be allowed

Inbound Permissions using Telnet, or Inbound using Rlogin. The time of day and days in which the user can access the network are the final items in the **User Permissions** dialog box. Once this is established for each user and the user database is loaded into the RASFinder, all the remote users can dial into the network and access the network resources according to the restrictions/permissions on this dialog box.

For example, Remote User2 (in our typical application) could initiate a dialup session by merely entering their User name and password in the Dial-Up Networking (My Connection) dialog box (see below) after having first set up a New Connection (called “My Connection”) and entering the phone number of RASFinder WAN port 2 (716-5429), which is assigned to User2.



Once Remote User2 has connected and been authenticated, they have access to the services on the LAN. For instance, if he/she wanted to print a report, it could be sent to the printer and printed out just as if Remote User2 was on the local area network.

Router Application

The second basic application for the RASFinder is LAN-to-LAN routing as shown in Figure 4-3. The RASFinder is initially configured for a RAS application. To configure the RASFinder for a router application, you have to change the WAN port addresses to be on a different network from the LAN port. The remote WAN ports have to be on the same network as the local WAN ports. Finally, you would have to change the Remote Port setup from a RAS application (Client only) to a routing application (Client or LAN). If your routing application would benefit from having all three WAN ports tied together to triple your WAN speed, then you would have to enable the MultiLink Point-to-Point protocol (MLPPP) option.

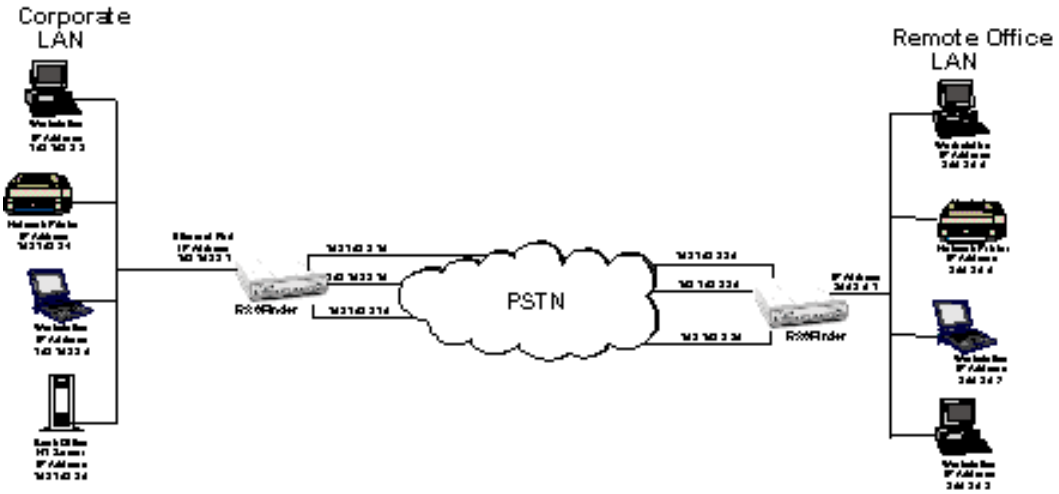
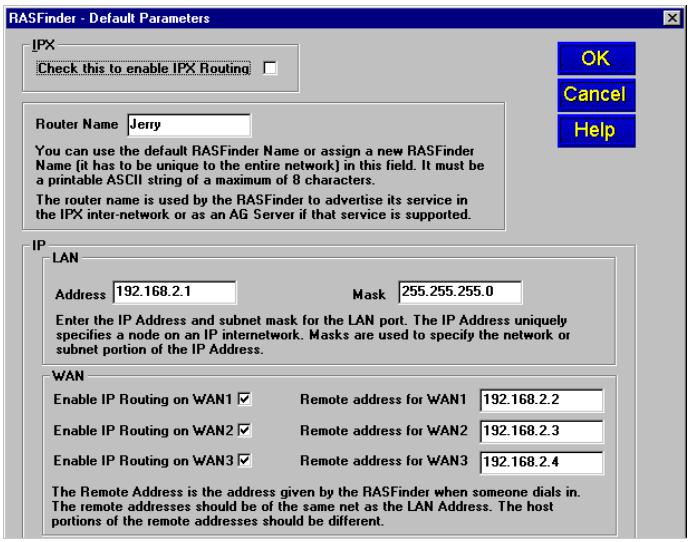


Figure 4-3. Router Application

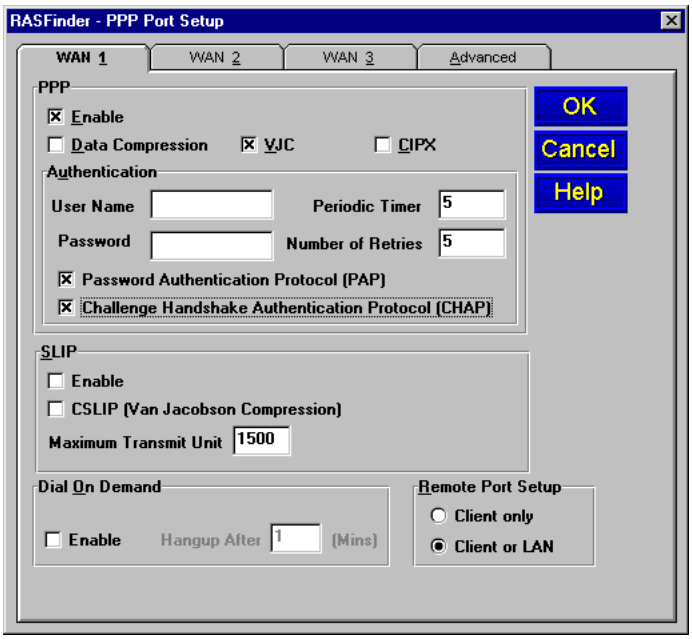
During initial software loading, you begin to configure the RASFinder for a routing application. A typical routing application is shown in Figure 4-3 and will be used as an example in the following discussion.


RASFinder - Default Parameters
IPX
Check this to enable IPX Routing
OK
Cancel
Help
Router Name
Jerry
You can use the default RASFinder Name or assign a new RASFinder Name (it has to be unique to the entire network) in this field. It must be a printable ASCII string of a maximum of 8 characters.
The router name is used by the RASFinder to advertise its service in the IPX inter-network or as an AG Server if that service is supported.
IP
LAN
Address
192.168.2.1
Mask
255.255.255.0
Enter the IP Address and subnet mask for the LAN port. The IP Address uniquely specifies a node on an IP internetwork. Masks are used to specify the network or subnet portion of the IP Address.
WAN
Enable IP Routing on WAN1
Remote address for WAN1
192.168.2.2
Enable IP Routing on WAN2
Remote address for WAN2
192.168.2.3
Enable IP Routing on WAN3
Remote address for WAN3
192.168.2.4
The Remote Address is the address given by the RASFinder when someone dials in. The remote addresses should be of the same net as the LAN Address. The host portions of the remote addresses should be different.

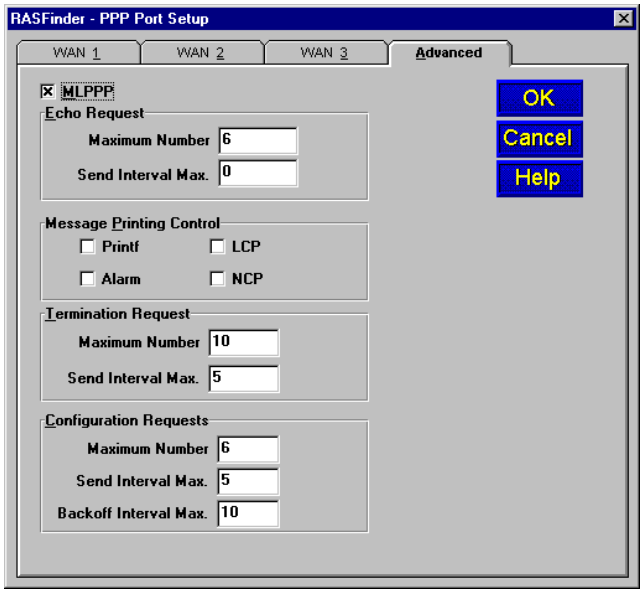
When you changed your LAN IP address in the **Default Parameters** dialog box to your unique LAN addressing structure and then try to change your Remote WAN port addresses to a different network which you need for your routing application, you set up RAS as the default configuration versus your router configuration. The Default Parameters dialog box will not allow you to change the addressing scheme of the Remote WAN ports to your unique addressing structure for your routing application. Therefore, you have to leave the Default Parameters dialog box set up for a RAS application initially (during initial software installation and configuration); then later, from the main menu, you can switch

from a RAS application to a routing application.

The PPP/SLIP (Point-to-Point/Serial Line Internet Protocol) button displays the **PPP Port Setup** dialog box with the WAN 1 tab active. In the Remote Port Setup group in the lower right of the dialog box, change from the Client only option to the **Client or LAN** (as shown below); this disables the **Client only** option, and enables the RASFinder to communicate with *either* a remote client (PC) or a LAN. The WAN 2 and WAN 3 tabs must have the **Client or LAN** enabled for both of these ports, too.



To bond the three WAN ports together, tripling the transfer rate between two LANs, click the Advanced tab and enable the **MLPPP** (MultiLink Point-to-Point Protocol) option. Then return to the main menu.



You must now decide which protocol your LAN is using and choose that protocol from the main menu. For example, to configure the RASFinder for IP, the Port IP Address and IP Mask fields in the IP Port Setup dialog box display the information that was entered earlier for your Default Parameters during initial software loading. When you click the IP Port WAN tabs, the RAS LAN IP address appears in the Port address field for the WAN ports. For a routing application, you have to change the Port IP Addresses so the LAN port has a different address from the WAN port addresses, and you may have to check that the WAN IP port addresses are identical (for MLPPP) and that the Remote IP Addresses of the Remote WAN ports are on a *different* network. If you are not using MLPPP, then you have to assign each WAN port a different address and ensure that the remote WAN ports are on a different network.

In our routing example (Figure 4-3), the Corporate LAN was set up with the Ethernet IP address 192.168.2.1 and the three WAN ports were given the IP address 192.168.3.10. Whenever they are assigned the same IP address, the WAN ports are added together and look as one to the PSTN, and the speed of the wide area network (normally the slowest cog in the system) is tripled to a value of up to 168 Kbps.

After making these changes, you are returned to the main menu where you need to download this new configuration to the RASFinder.

To set up the remote office LAN, go through the same process except point the WAN ports toward the Corporate LAN. The remote WAN ports could be set up with an IP address of 192.168.3.20. When this is accomplished, users at the remote office can receive their e-mail from the Corporate file server and print their e-mail on their local printers.

IP Setup

The **IP Port Setup** dialog box enables you to change the IP routing capabilities that were set up during software installation. This dialog box has five tabs: Ethernet, WAN 1, WAN 2, WAN 3, and Advanced.

The **Ethernet** tab enables you to configure various parameters relating to the Ethernet port. For example, you can change the Ethernet port IP Address and IP mask; If necessary, you can change the Ethernet Frame Type from Type II to SNAP; you can enable or disable various types of support, set up RIPv2 parameters, and enable the type of Authentication (if any).

The **Frame Type** option defines the MAC layer frame encapsulation to be used for IP transmissions from the specified port. The Ethernet port supports Type II and SNAP frames, but the WAN ports support only Type II frames.

In the **Support** group, **ICMP Redirect** defines if the specified port is permitted to issue an ICMP Redirect message to the source IP address. The most likely cause of this message is the delivery of a datagram to a router that is not on the forwarding path to the destination address. This is often due to a wrong configuration of the IP client sending the datagram. The packet causing the ICMP Redirect message to be transmitted is forwarded to the appropriate router.

ICMP Mask Reply enables support for nodes on the connected networks to learn their subnet masks.

RIP (Routing Information Protocol) enables RIP-based routing on the specified port, and is normally enabled. However, RIP can be disabled if you are using WAN links in Dial-on-Demand mode. In such links, disabling RIP will reduce traffic on the link as this will also disable periodic RIP broadcasts. RIP routing on the port will be automatically turned off when Dial-on-Demand is enabled in PPP port setup.

Finally, the **RIP Poisoned Reverse** option defines if Poisoned Reverse RIP messages are supported on the specified port. Generation and processing of poisoned routes (RIP entries with their respective metric set to 16 (defined as infinity) is enabled/disabled by this parameter. Poisoned reverse is a method used by RIP to improve the rate of convergence of the routing tables of interconnected IP routers. Routers supporting poisoned reverse that receive such RIPs ignore the entries set to 16 and thus prevent the propagation of unnecessary (and often incorrect when a topology change occurs) information which in turn speeds up the rate at which RIP will correctly map the current network topology.

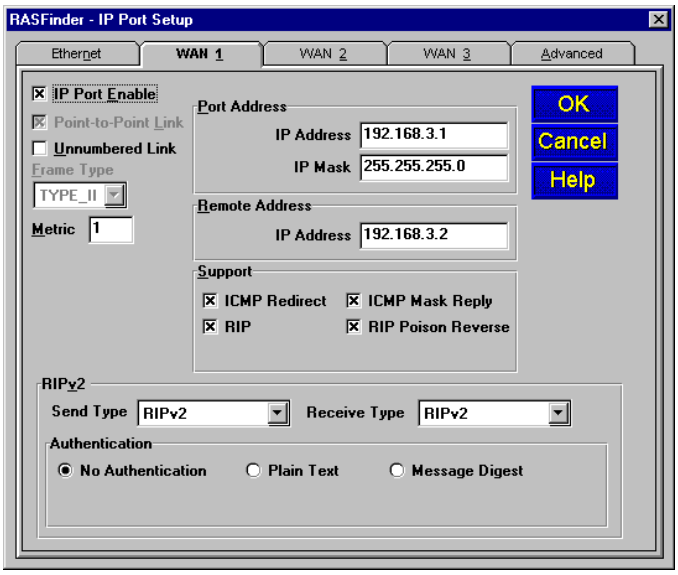
Routing Information Protocol, Version 2 (RIPv2)

RIPv2 has enhanced “explicit” netmask information and supports several new features including external route tags, subnet masks, next-hop addresses, and authentication. Subnet mask information makes RIP more useful in a variety of environments and enables the use of variable subnet masks on the network. Support for next-hop addresses permits the optimization of routes in an environment that uses multiple routing protocols. For example, when RIPv2 is being run on a network along with another IGP, and one router is running both protocols, then that router can indicate to the other RIPv2 routers that a better next-hop than itself exists for a given destination.

RIPv2 packet setup is accomplished at the bottom of each of the WAN tabs. The **RIPv2** group enables you to set up the send and receive packet types as either RIPv2 (default), RIPv1 Compatible, or None. You can also set up RIPv2 authentication here.

The **Authentication** subgroup is the RIPv2 mechanism for authenticating the sender of the routing eliminates the vulnerability of the routing infrastructure. This authentication scheme is essentially the same mechanism provided by OSPF. Currently, only a plain-text password is defined for authentication.

For Plain Text RIPv2 authentication, the maximum length of the password is 16 characters; however, Message Digest authentication can have a key id field of up to 50 characters.



On the WAN port tabs you can change any parameters that are active, including most of those discussed (above) for the Ethernet tab plus the WAN IP Port Enable, Unnumbered Link, and the Remote IP Address.

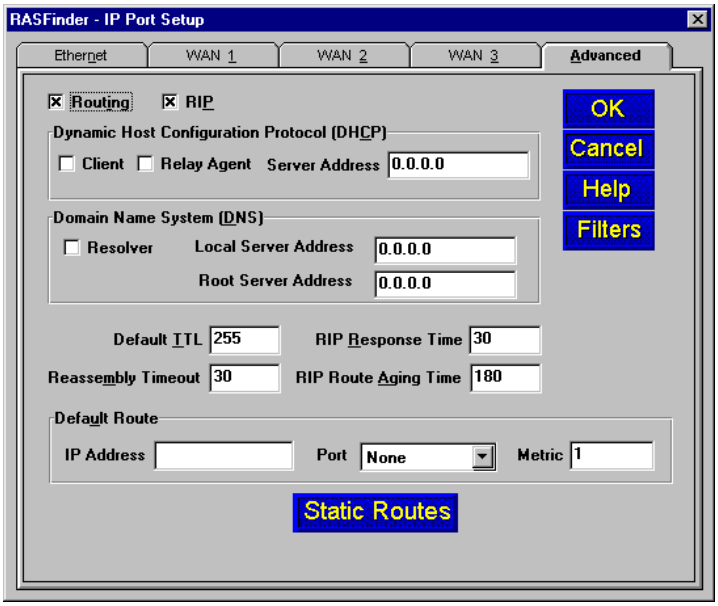
WAN 1, WAN 2, and WAN 3 Tabs

If you enable the IP routing master control on the Advanced tab but disable the control on this tab, all IP packets received or to be transmitted on this WAN port will be discarded. Even if bridging is enabled, the packets will not get across the link.

The **Unnumbered Link** option can be selected (checked) for the WAN ports for point-to-point links. When selected, it disables the Port Address and Remote Address groups. Unnumbered links are useful only between two routers; in this case, local and remote. When running RIP over a PPP link, both ends of the link must be either unnumbered or numbered with the same IP subnet. An advantage of not assigning an IP address to each WAN port is that you conserve valuable network and subnet numbers.

Remote IP Address defines the IP address for the destination end of a point-to-point link and is necessary only if the selected WAN port has been enabled for point-to-point operation. Note that the

remote IP address must fall within the same IP network as the local WAN IP address.



The **Advanced** tab is used to enable IP routing and RIP authentication and defines how the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers are to be used. This tab is also used to set up the default route, any filters, OSPF (Open Shortest Path First), and Static Routes. This tab also enables you to set up various configuration options for IP routing protocol, and any options selected here apply to all ports on which IP routing takes place.

The **Routing** option is normally checked; however, if you do not wish to have IP packets routed, then uncheck this item. If IP routing is disabled and bridging is enabled, IP packets are bridged; i.e., IP packets are transferred.

The **RIP** option enables RIP based routing. RIP (Routing Information Protocol) is a protocol used among routers to exchange routing table information. RIP is the most common protocol used in both IP and IPX networks. It is also used internally by client workstations in IPX networks to obtain routes (shortest, or otherwise) to any distant network. RIP based routing should normally be enabled. It can be disabled, however, if you are using WAN links in Dial on Demand mode. For DOD links, disabling RIP will reduce traffic on the link as it will also disable periodic RIP broadcasts. RIP routing on a given port will be automatically turned off when Dial on Demand is enabled on the PPP Port Setup tab for the WAN port.

The **DHCP (Dynamic Host Configuration Protocol)** group enables you to set up the WAN ports as client-only. Then, a PPP client connected to the WAN port will be on the same IP network as the LAN port of the RASFinder. This feature can save some extra IP addresses that otherwise would have been taken up by the WAN port. Enabling the Client option allows the RASFinder to dynamically get an IP address for a PPP client coming up on one of its “Client-only” WAN ports. When this option is enabled, there must be a DHCP server or a DHCP relay agent on the connected LAN in order for the RASFinder to acquire an appropriate IP address.

In most cases, you should not have to change any of the timers (i.e., default TTL, reassembly time-out, RIP response time and RIP route aging time).

When the router is configured for remote access, the DNS Resolver needs to be enabled so that applications such as the terminal server will support Domain Names. The dotted decimal IP address of the Local DNS server should be entered in the field provided.

The **Static Routes** feature enables a remote network PC to access a specific workstation or peripheral device on another network through a predefined route (static route). Static routing is

normally used when a part of an internetwork can be reached by only one particular path. Static routes are manually configured routes that specify the transmission path a data packet must follow based on the data packet's destination address. A static route could enable a client pc on the manufacturing network to send a document to the printer on the corporate network. This static route is shown in the top network in Figure 4-4. A static route can also use an unnumbered link to provide a particular route from a remote client device to a specific device on another network. The unnumbered link is shown in the middle network in Figure 4-4.

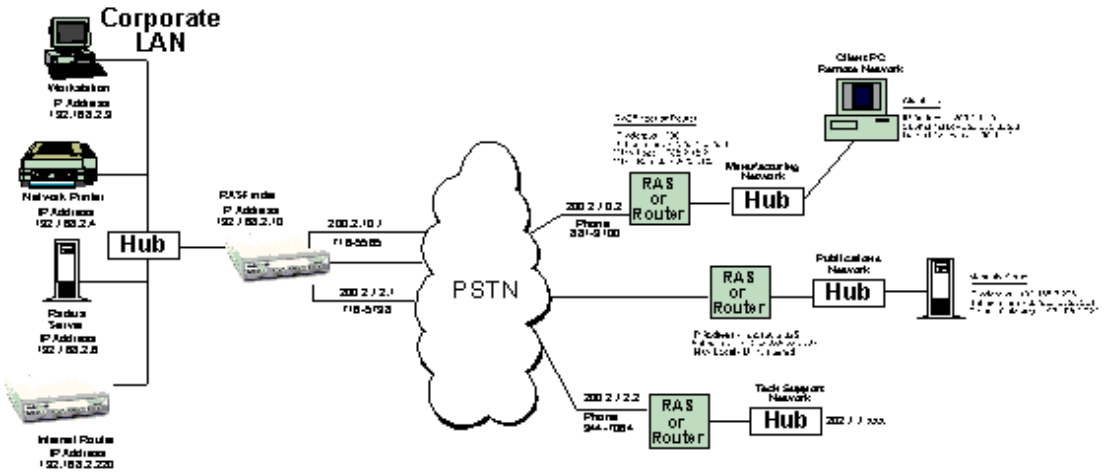
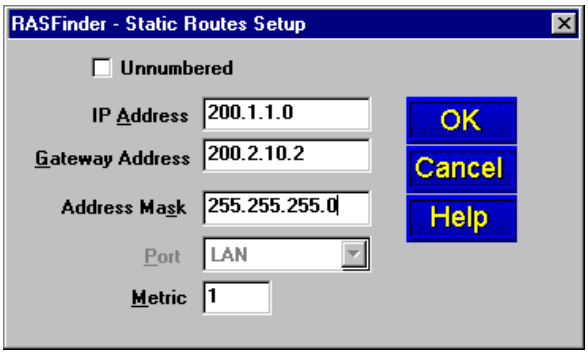


Figure 4-4. Static Routes

In our first example above, where a data packet from the remote client PC on the manufacturing network is being sent to the corporate printer, the Static Routes Setup dialog box would contain an address of 200.1.1.0 in the IP Address field and a gateway address of 200.2.10.2. The **Unnumbered** option would be left unchecked in this example. The **IP Address** field contains the address of the target host or network, a PC on the manufacturing network. The **Gateway Address** is the address of the local router on the manufacturing network (200.2.10.2) on the next hop toward the target host. The **Address Mask** is the IP subnetwork mask (255.255.255.0) of the target host. The **Port** field is inactive, greyed out in this example. **Metric** is the hop count (1) to the target host.

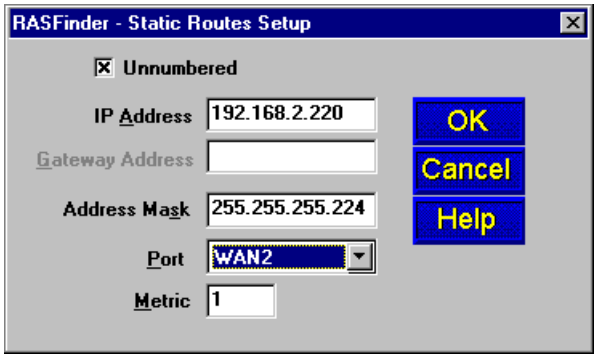


Now, for our second example of an unnumbered link where we want a server on a remote network to appear as a device on a router on the corporate LAN that is pointed toward the Internet. Let say that the Manuals Server on the Publications Network contains the released manuals that a customer can down load from the corporate network. So in order to have the Manuals Server appear on the Internet, we need to set up the corporate RASFinder with an unnumbered link and for the purposes of our example, lets use WAN 2. Also, the Internet router on the Corporate LAN will have a default route of 192.168.2.224 with a subnet Address Mask of 255.255.255.224, and a Gateway Address of 192.168.2.10.

So, for this application to work, you need to set up a default route on the Corporate RASFinder of

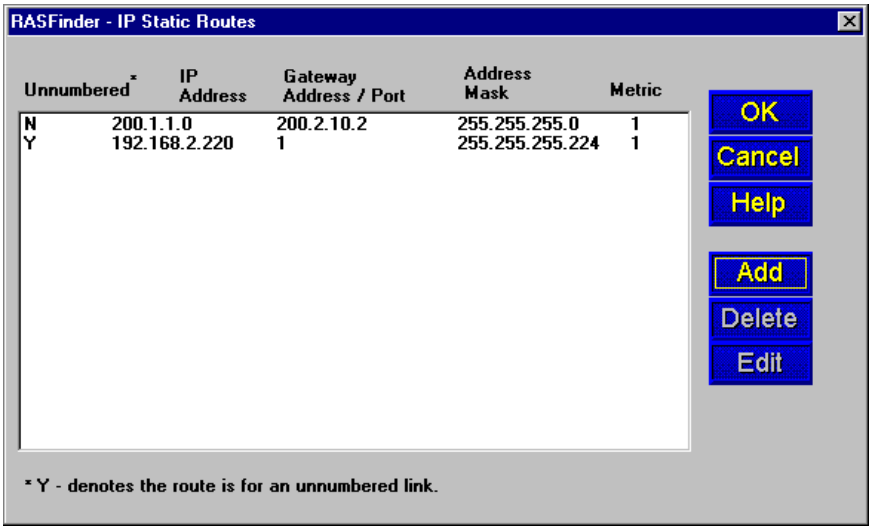
192.168.2.220 which is pointing at the Internet router. You then, need to go into the IP Port Setup dialog box, select the WAN 2 tab, and activate the Unnumbered Link option. When you do this, the Port Address and the Remote Address groups become inactive. You should turn off RIP in the Support group on WAN 2 so that the RASFinder does not try to broadcast RIP packets which take up unnecessary bandwidth. Then you need to check the PPP/SLIP button on the Main menu and ensure that the Remote Port Setup group for WAN 2 is set to Client or LAN.

Now go back to the IP Port Setup dialog box and hit on the Advance tab, then click on the Static Routes button. This brings up a blank IP Static Routes dialog box, hit on the Add button to bring up the Static Routes Setup dialog box and when you enable the Unnumbered option, the Port option becomes active and the Gateway Address option becomes inactive.



Now, for the IP Address field we want the address of the Internet router on the Corporate LAN which in our unnumbered example is 192.168.2.220. In order for the Manuals server on the Publications network to appear on the Corporate LAN, we need to subnet the Manuals server with an Address Mask of 255.255.255.224. The Port option identifies the WAN port on the Corporate RASFinder that is unnumbered. In our example, WAN 2 is the port. The Metric hop count remains at one (1).

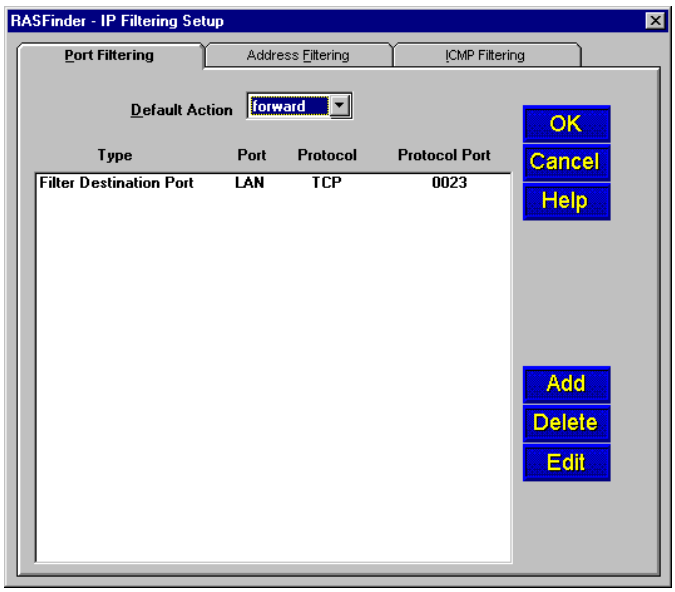
When we click on the OK button for the Static Routes Setup dialog box, the IP Static Routes dialog box now displays the two examples of static routes.



To complete the Static Route application, the Publications network RASFinder or router, depending on the type of device used on the network would need a default route of 192.168.2.226 that is looking at the Manuals Server. The Ethernet port IP address could be 192.168.2.225 with a net mask of 255.255.255.224.

Filters

The network administrator can set up filters on the RASFinder for better control. Filtering can be used when you want to block all packets originating from a specific destination (called source address filtering) or all packets heading for a particular destination (called destination address filtering). Filters can be set up to exclude packets of a particular protocol (TCP or UDP) or any particular field in a LAN packet. The **IP Filtering Setup** dialog box lists the port, address, or Internet Control Message Protocol (ICMP) filtering for the IP protocol.



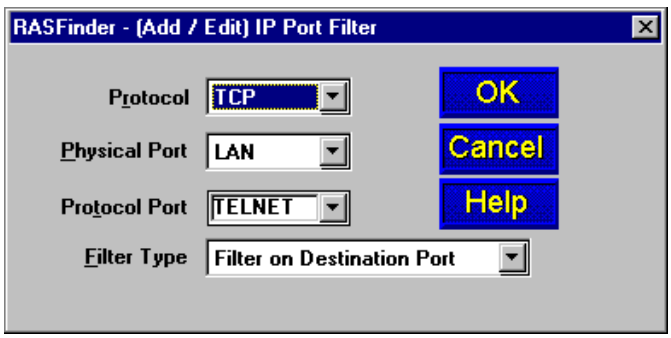
Initially, the filtering list window, i.e., the window area that displays the Type, Port, Protocol, and Protocol Port information is blank. This information displays in the window when the Add/Edit IP Port or Address Filter dialog box is filled out.

Note: When filters are installed, the RASFinder needs to do extra processing (i.e., it needs to look into each packet that has to be routed or bridged). Thus, installing too many filters may lead to performance degradation.

Port filtering filters or forwards IP packets based on their specific purpose; i.e., whether they are Telnet (TCP based) or TFTP (UDP based) packets. Address filtering filters or forwards packets based on their source or destination IP address. Separate filtering support is provided for specific kinds of received ICMP packets.

The filtering list window on the Port Filtering tab (above) displays the filter Type, the physical Port (LAN, or one of the WAN ports), the Protocol (TCP or UDP), and the Protocol Port. On the Address Filtering tab (not shown), the Protocol and Protocol Port columns are replaced by IP Address.

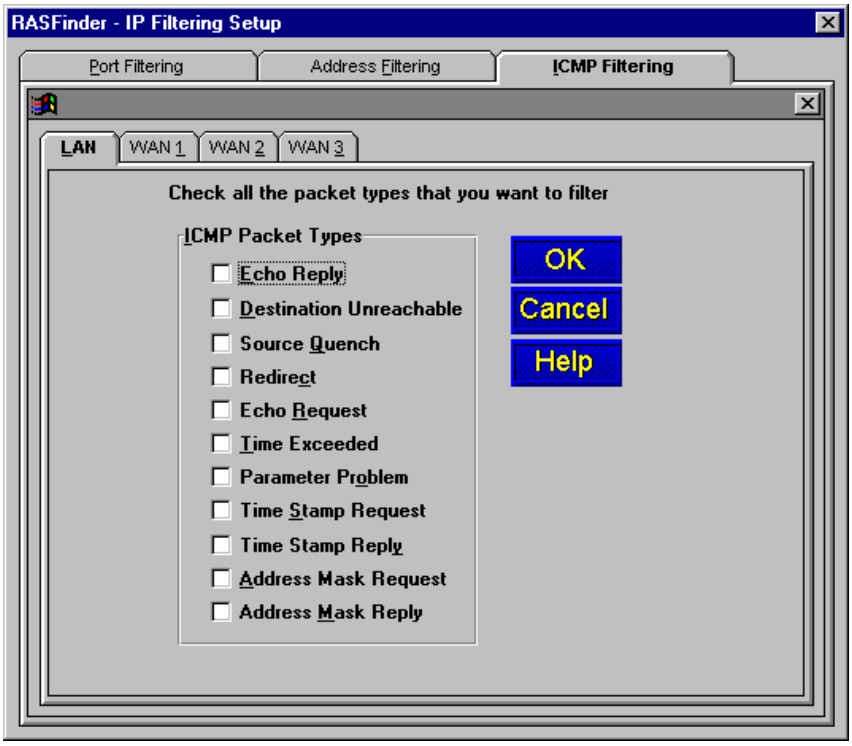
To add or edit a filter listing, the **Add/Edit IP Port (Address) Filter** dialog box is used. This dialog box enables you to create an entry which is then displayed in the filtering list window. In the example



Add/Edit IP Port Filter dialog box, the protocol that is going to be filterred is TCP, the physical port on which the filtering is going to take place is the LAN port, the protocol port is telnet which translates into protocol port number 0023 in the filtering list window, and the filter type is Filter on Destination Port which means to drop all IP packets whose destination protocol port is telnet.

Address filtering uses the IP address in the IP Address field (example, packets with address 192.168.2.40), applies filtering to the physical port listed in the Physical Port field (LAN), and if the Filter Type is Filter on Destination Address that means that all packets with an IP address of 192.168.2.40 that are destined for the LAN port are blocked.

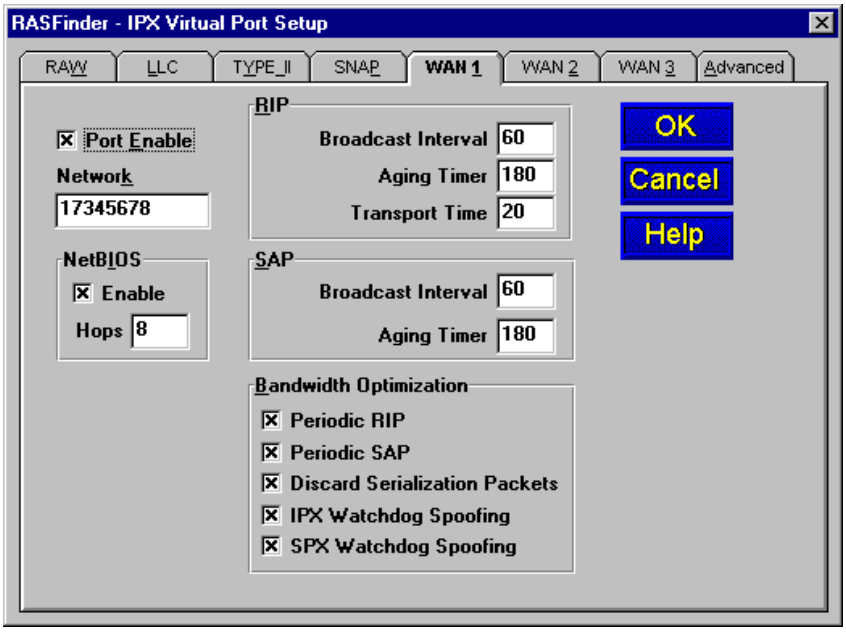
ICMP filtering provides separate filtering support for specific kinds of received ICMP packets. ICMP filtering is used in IP networks as an internal protocol for nodes to exchange control and diagnostic information. Applications normally do not use ICMP filtering for any purpose.



You can select ICMP filtering on your LAN or WAN ports and the type of filtering on each port by choosing the filtering type from the ICMP Packet Types list.

IPX Setup

The **IPX Virtual Port Setup** dialog box is used to control the four frame types and set up the three WAN ports of the RASFinder. The Advanced tab opens an IPX general setup window used to enable or disable IPX routing and autolearn of Ethernet network numbers; also, the distributed name of the RASFinder can be designated here.



In IPX based networks using Ethernet, LAN segments can support the use of four different Ethernet frame formats over the same physical link (provided each frame type has a unique network address as a virtual port).

The three WAN tabs allow you to enable or disable IPX routing on the WAN ports, change the network numbers for the WAN ports, change the default RIP and SAP timers, and optimize the bandwidth. The IPX WAN network number has to be the same on both ends of the link and must be unique throughout the internetwork. If a WAN port is configured in a point-to-point operation, both WAN network numbers have to be the same and unique.

NetBIOS, when enabled, enables the transport of Novell encapsulated NetBIOS packets on the specified virtual IPX port. Refer to Novell documentation regarding NetBIOS operation over NetWare based LANs. The Hops text box defines the distance, in hops, for the routing of Novell encapsulated NetBIOS frames on the specified virtual IPX port, and the recommended value is 8.

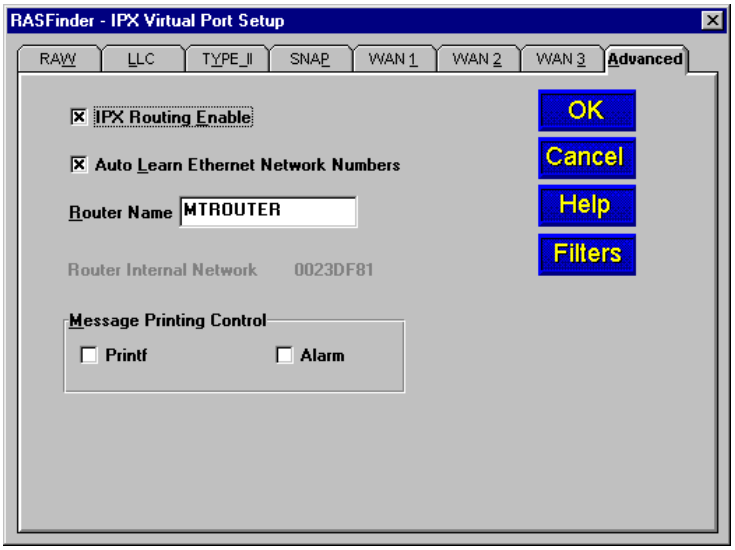
Periodic **RIP** (Routing Information Protocol) refers to broadcasts transmitted from the RIP virtual IPX port at a given frequency so all routers on the internetwork maintain consistent routing tables. Increasing the frequency of RIP broadcasts can consume excessive bandwidth, especially on low-speed WAN links. Sixty seconds is the recommended interval between RIP broadcasts. The default RIP timer settings should work well for most applications.

Periodic **SAP** (Service Advertisement Protocol) is used in IPX based networks to enable servers (application servers, file servers, print servers, communication servers, etc.) to advertise their presence on the internetwork. Routers use these advertisements to build up tables listing the servers so they can then advertise these servers on the local segments and provide routers to the server. Client workstations can request a list of these servers from the router. The default SAP timer settings should work well for most applications.

Bandwidth Optimization Group

Discard Serialization Packets, when enabled (checked), causes the IPX router to discard Novell Netware File Server serialization security frames received from the specified virtual IPX port. Novell Netware File Servers implement broadcast frames, often referred to as security frames, that contain serialization information regarding the license of the file server executable. This feature permits filtering of these broadcasts to help reduce WAN traffic and is not intended to interfere with copyright protection mechanisms. This feature is automatically turned on when Dial-On-Demand is enabled in PPP port setup.

The Advanced tab controls the master routing of the protocol and auto learn of Ethernet network numbers, defines the broadcast name of the RASFinder, and enables IPX filtering.



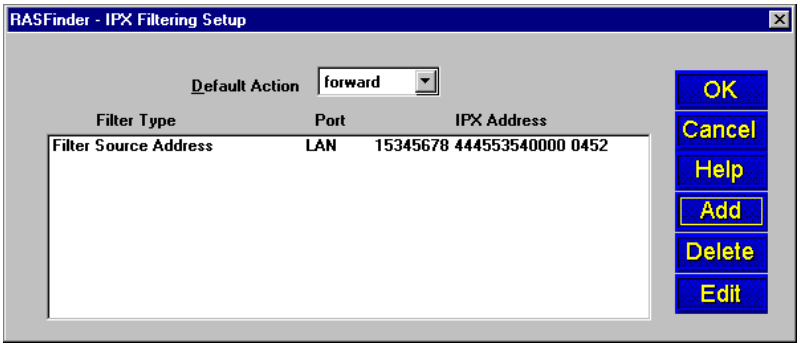
If bridging of IPX packets is desired, IPX routing must be disabled and frame type support for the frame type must be enabled.

If there is a server on the local segment, then IPX network number auto learn should be enabled. If there is no server, or if for some reason the RASFinder comes up before the server does, the RASFinder will default to some random network numbers after a short period of time.

IPX Filters

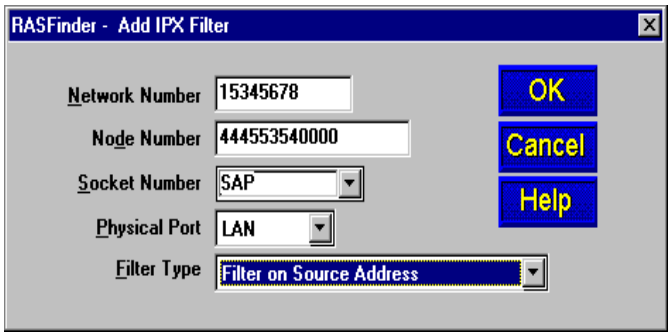
The network administrator can set up filters on the RASFinder for better control. IPX packet filtering can be set up to selectively filter or forward packets based on the IPX address.

Filtering can be used when you want to block all packets originating from a specific destination (called source address filtering) or all packets heading for a particular destination (called destination address filtering). Filters can be set up to exclude packets of a specific port. The **IPX Filtering Setup** dialog box lists the filter type, port, and IPX address. Initially, the filtering list window, i.e., the window area that displays the Filter Type, Port, and IPX Address information is blank. This information displays in the window when the Add/Edit IPX filter dialog box is filled out.



Note: When filters are installed, the RASFinder needs to do extra processing (i.e., it needs to look into each packet that has to be routed or bridged). Thus, installing too many filters may lead to performance degradation.

The Add or Edit IPX Filter dialog box allows you to enter a network number and node number, and define a socket number, physical port, and filter type. The Network Number defines the physical port which is defined by turning off AutoLearn Ethernet Network Numbers option in the IPX Virtual Port Setup dialog box under the Advanced tab. The Node Number is a 12-digit alphanumeric MAC



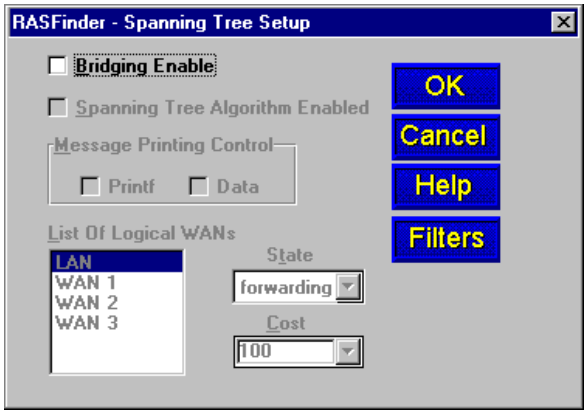
Address of the Ethernet NIC that is providing your Ethernet interface. The Node Number is defined in the IP Configuration dialog box under the Adapter Address in the Ethernet Adapter Information group. The Adapter Address is presented with dashes between each set of two alphanumeric digits. These dashes can not be used in the Node Number. The IP Configuration dialog box is accessed from a DOS prompt by enterring winipcfg.

The socket number, physical port, and filter type are provided in drop down lists. Three socket number selection are provided; NCP, RIP, and SAP. The physical port lists the available port for which filtering can be accomplished; LAN and the three WAN ports. The filter type defines whether you are going to forward or filter depending on the source or destination address.

Spanning Tree Setup

This dialog box lets you configure the parameters for transparent bridging or bridging using Spanning Tree Algorithm as specified in IEEE 802.1d standard. Transparent bridging occurs between two remote Ethernet LANs.

Spanning Tree Algorithm is a protocol specified by the IEEE 802.1d standard for use by bridges to perform bridging. Bridges implementing this protocol interact with each other so as to prevent bridging-loops in an internetwork with redundant links to the same networks. This algorithm also allows for automatic use of alternative routes (provided there are redundant paths to the destination) in case the original route is unavailable for some reason.

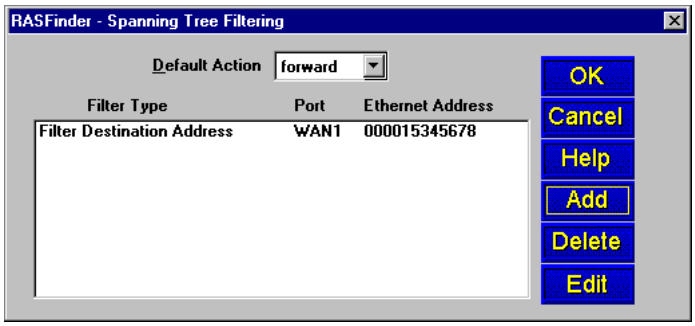


Bridging needs to be enabled to support networking protocols such as NetBIOS. However, if you are using only IP and IPX, the RASFinder will operate more efficiently if you leave bridging disabled.

With Spanning Tree bridging, the default initial state of each port in the **List Of Logical WANs** is “forwarding.” Other available options include: “listening,” “learning,” “blocking,” and “disabled.” Cost (or Path Cost) indicates the relative cost of using a given port to bridge to a remote network and is defined as 1,000 divided by the megabit data rate of the Network connected to the specified port. The default value for the LAN port is 100, and the value assigned for each of the WAN ports is 1000.

The **Filters** button enables the construction of a filtering database. Packets whose Ethernet source address or destination address is not found in the filtering database will either be filtered or forwarded, depending on the setting of the **Default Action** field, with a default setting of “forward.”

Filtering can be used when you want to block all packets originating from a specific destination (called source address filtering) or all packets heading for a particular destination (called destination address filtering). Filters can be set up to exclude packets of a specific port. The **Spanning Tree Filtering Setup** dialog box lists the filters by filter type, port, and Ethernet address. Initially, the filtering list widow, i.e., the window area that displays the Filter Type, Port, and Ethernet Address information is blank. This information displays in the window when the Add/Edit Spanning Tree Filter dialog box is filled out.



Note: When filters are installed, the RASFinder needs to do extra processing (i.e., it needs to look into each packet that has to be routed or bridged). Thus, installing too many filters may lead to

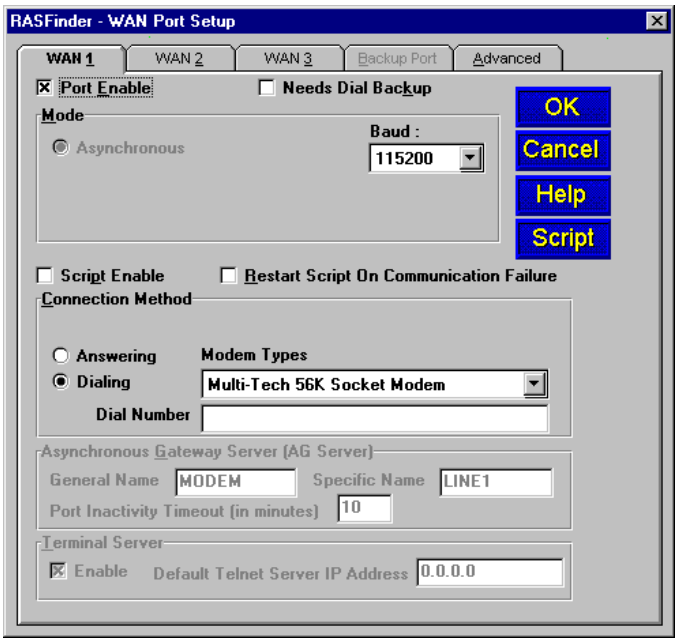
performance degradation.

The add or edit **Spanning Tree Filter** dialog box allows you to enter the Ethernet address (for example 15345678) to which you want to apply filtering, the physical port (WAN 1) on which the filtering is going to be applied, and the filter type in our example of Filter Destingation Address.

This means that all packets with a destination address of 15345678 going to WAN 1 are dropped.

WAN Port Setup

The **WAN Port Setup** dialog box controls how each WAN port is configured. Since each port has a built-in modem, the default Mode, “Asynchronous” cannot be changed. The **Connection Method** can be set to either **Answering** or **Dialing**. If **Dialing** is enabled, then the number to be dialed has to be entered in the **Dial Number** field. The entry **Multi-Tech 56K Socket Modem** in the **Modem Types** field refers to the built-in modem installed in the RASFinder.



If either WAN 1 or WAN 2 needs dial backup in case it loses carrier (i.e., the Carrier signal, DCD, goes down), then WAN 3 can be used (dedicated) for this purpose. The **Needs Dial Backup** check box on the appropriate WAN tab (WAN 1 or WAN 2) must be enabled, then the dial backup number must be entered on the **Backup Port** tab (after it is active); when it is used for backup, WAN 3 will no longer be available for routing or RAS.

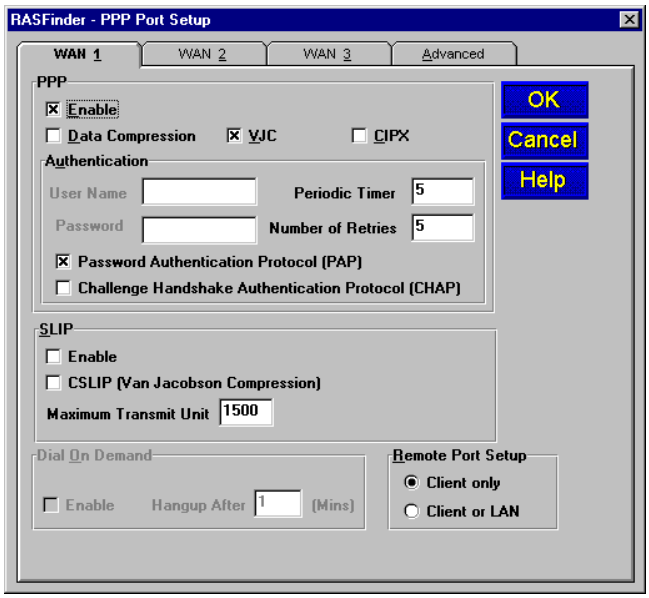
The **Script** button provides access to the scripting options. The **Script Dialog** menu enables you to edit, compile and download scripts. A script file (a text file containing a sequence of commands; refer to Appendix B) can be used to automate certain RASFinder operations. The **Script Enable** or **Restart Script On Communications Failure** option can be used to either start scripting or restart a script upon failure.

The RASFinder has built-in support for Multi-Tech Communication Services Interface Server (MCSI, NASI, NCSI, or AG server) if every asynchronous communication line across the internetwork has a unique MCSI name. If you set the Connection Method for **Answering**, the **Asynchronous Gateway Server (AG Server)** group becomes active, enabling you to set the General Name and Specific Name of the interface corresponding to that specific Port (WAN 1, WAN 2, or WAN 3). The name of the AG Server is assumed to be the same as the IPX router name (or at least the first eight characters of the Router Name entered on the IPX Advanced tab). The **General Name** can be any 8 alphanumeric characters (with no question marks) and the **Specific Name** can be any 14 alphanumeric characters (with no question marks).

Setting the Connection Method for **Answering** also activates the Terminal Server group, where you need to enter, in the field provided, the dotted decimal IP Address of the default Telnet server.

Point-to-Point Setup

The **PPP Port Setup** dialog box controls the WAN port protocol, dial on demand, and remote port setup. The WAN port protocol can be either Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP). Of these two protocols, PPP is the more robust as it enables the endpoints to negotiate the use of the link and protocol parameters in a standardized way and also enables for standardized encapsulation of the packets. SLIP is an older protocol which requires manual authentication using a script.



PPP is the default protocol. The PPP software in the RASFinder internally negotiates the use of a suitable authentication protocol (PAP or CHAP) with the remote router or remote access client software. When either PAP or CHAP (or both) is enabled, the RASFinder expects the peer (the client on the other side of the WAN link) to be configured with a User Name and Password combination that is in the RASFinder's User Database. The User Name and Password are both ASCII character strings that can be up to 30 characters long. However, for router-to-router connections, authentication is normally not used and the User Name and Password fields are empty.

The **Periodic Timer** option shows the interval between authentication checks. The recommended value is 10 seconds. The **Number of Retries** option, with a recommended value of 5, refers to the number of retries during each PAP or CHAP authentication check.

If SLIP is to be used on one of the WAN ports, then select the SLIP Enable option on the corresponding tab and PPP will be disabled automatically. If the TCP/IP header is to be compressed using VJC compression, then check the **CSLIP (Van Jacobson Compression)** option. (Note: on answering WAN ports, the RASFinder can detect the type of connection -- PPP or SLIP.)

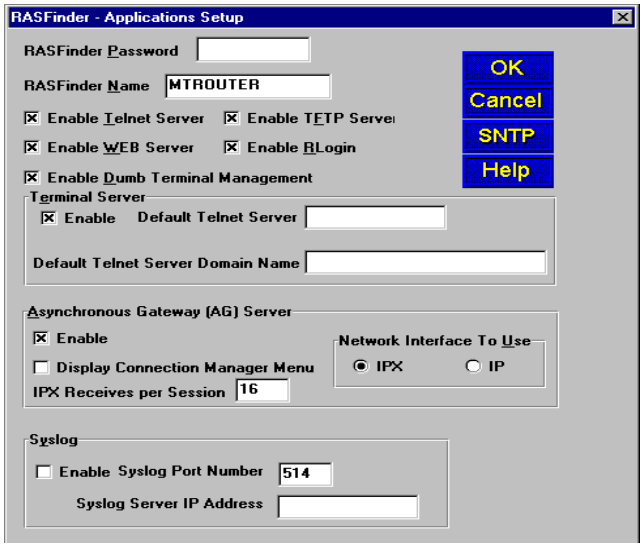
You can set up the RASFinder to bring down the connection on the WAN link when there is no real data traffic on the line; the router will then automatically bring up the WAN link when data is available to go across the link.

In the **Remote Port Setup** group, the **Client only** option saves IP addresses in a RAS application because the remote node (a dial-in client) becomes a virtual extension of the Ethernet LAN. For Routing, however, you must check the **Client or LAN** option, in which case there will be no saving of IP addresses on the WAN ports.

Applications

In addition to local configuration, the RASFinder supports various applications that enable remote viewing and changing of the configuration from anywhere on the connected internetwork. To manage these applications, click **Others** on the **Router Setup** menu.

The **Applications Setup** dialog box appears.

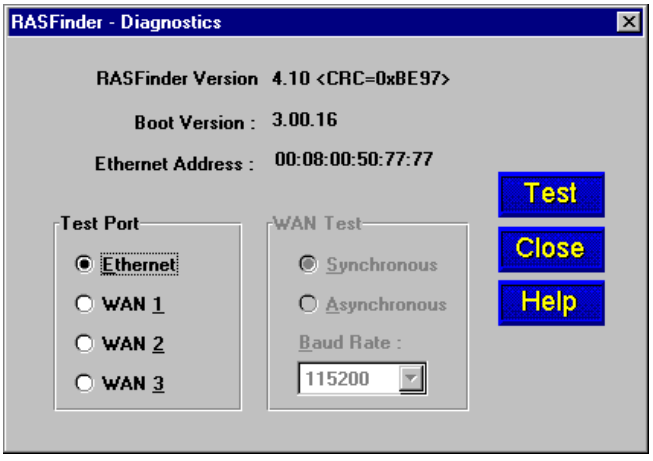


Verify that the desired applications are enabled (checked). The default condition is all applications are checked. To disable a given application, click to uncheck the check box and disable support.

For more information on using these remote configuration applications, click the on-line **Help** button or refer to Chapter 7, Remote Configuration and Management.

Diagnostics

The RASFinder is equipped with a built-in diagnostics utility that can be accessed by a PC cabled directly to the command port (remote users cannot access the diagnostics). Click the **Built-in Test** button on the **RASFinder Setup** menu and the **Diagnostics** dialog box displays.



In the **Test Port** group, select the port (Ethernet, WAN 1, WAN 2, or WAN 3) you want to test, then click the **Test** button to start diagnostic testing.

For additional details and parameters about specific fields in the **Diagnostics** dialog box, click the on-line **Help** button.

Client

The information provided in this section enables multiple users to configure their PCs to access the LAN through a RASFinder. The RASFinder was configured by the administrator who, while installing the software, determined that the RASFinder would either automatically assign Internet (IP) addresses, or require that they be assigned manually to each client PC. Also, the administrator assigned an IP address to the RASFinder's Ethernet port, and assigned user names and passwords to the WAN links. All these factors play a role in client configuration. Make certain that you are aware of the decisions made prior to setting up client PCs.

PC

To access the RASFinder, your PC must have communications capability including hardware such as a Dial Up Network Adapter/modem and any necessary software.

Make certain that your Dial Up Network Adapter IP addressing is dynamically assigned (default). If it is, then the only information you may be required to obtain is the IP address of your organization's Domain Name Server (DNS) - if DNS has been enabled on the **IP Setup** dialog box, Advanced tab.

Note: In cases where the IP address has been manually assigned, you will need to know the IP address of the RASFinder (Gateway address) in addition to the organization's Domain Name.

Checklist

A checklist is included so that you can record all the pertinent information required for the connection between your PC and the RASFinder. Keep this as a reference for future upgrades.

Use the following checklist to record all the configuration settings for future use:

Configuration Checklist	
IP Address (PC)	. . .
IP Address (RASFinder)	. . .
Host (User Name)	
Domain	
DNS Server Address	. . .
Network Adapter (Manufacturer/Model Number)	

RASFinder™
Remote Access Device

Chapter 5 - RAS Dial-Out Redirector

MultiTech® Systems

Introduction

Multi-Tech's Remote Access Server for Microsoft network users enables users to dial-out and fax-out through your MTASR3-200. Remote Access Solution software uses Multi-Tech's Communications Services Interface (MCSI - pronounced "Mik-see"). MCSI is a software redirector which complies with MCSI/NCSI/NASI defacto standards for software redirection.

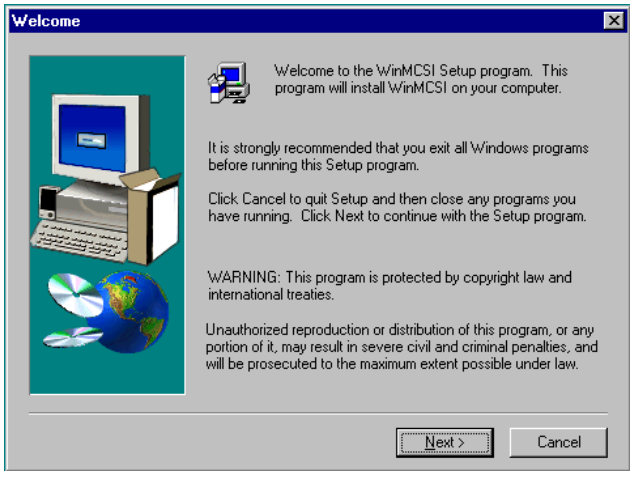
The Windows© version of MCSI, called WINMCSI, is supported on Windows 98 and NT platforms. MCSI2000 is supported on Windows 2000 and XP operating systems. MCSI 2000 is documented in a separate sofware installation guide on your product CD. Refer to the Multi-Tech Communication Serial Interface for Windows 2000 and XP Software installation Guide for information on MCSI2000.

Since WINMCSI provides data communications connectivity, it needs to be installed and operating before your data communications application software is started.

Installing and Configuring the WINMCSI Modem-Sharing Software

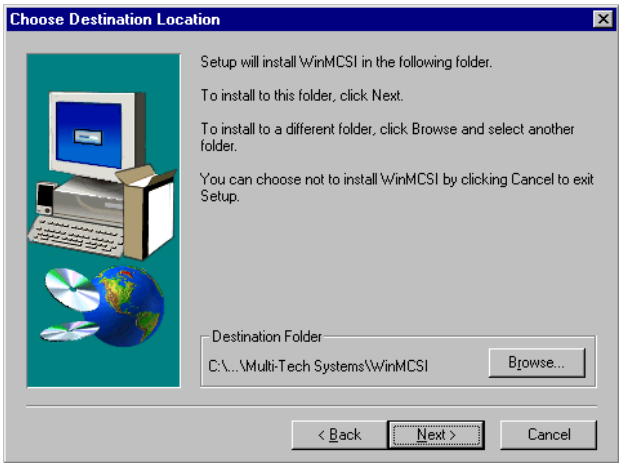
The WINMCSI modem-sharing software (included on the CD) manages access to an Asynchronous Gateway (AG) for outbound calls. It allows Windows communications software packages that do not support INT6B or INT14 to connect to a gateway. It also detects other compatible communications servers (e.g., RASs) on your network and displays the resources they provide to eligible LAN users.

1. Power on your client PC and log in to your LAN.
2. Start Windows.
3. Insert the Multi-Tech RASFinder CD into your CD-ROM drive. The **RASFinder** Splash screen displays.
4. Click on **Install MCSI Utility** button. A second window opens, choose the Windows operating system you wish to install.
5. The **Welcome** screen displays.


Welcome
Welcome to the WinMCSI Setup program. This program will install WinMCSI on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Next >
Cancel

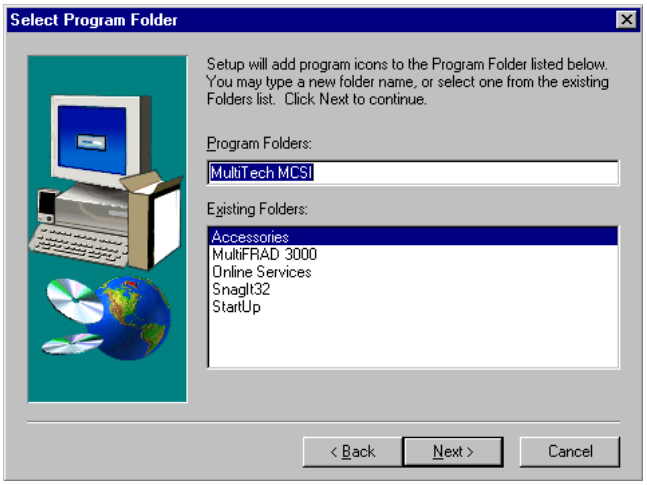
Click **Next** to proceed with the installation.

6. The **Choose Destination Location** screen displays.


Choose Destination Location
Setup will install WinMCSI in the following folder.
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
You can choose not to install WinMCSI by clicking Cancel to exit Setup.
Destination Folder
C:\...\Multi-Tech Systems\WinMCSI
Browse...
< Back
Next >
Cancel

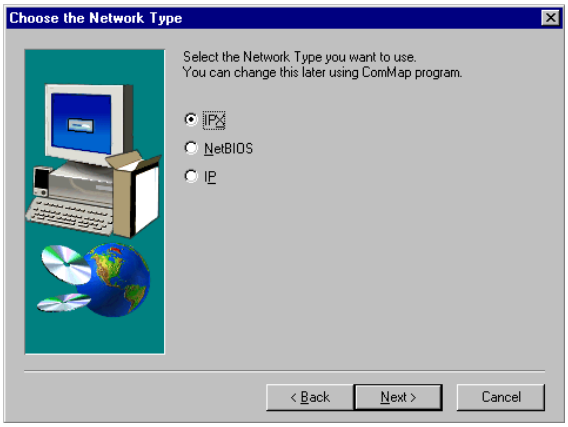
Click **Next** to accept the Destination Folder, or click **Browse** to select a different destination.

7. The **Select Program Folder** screen displays.


Select Program Folder
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.
Program Folders:
MultiTech MCSI
Existing Folders:
Accessories
MultiFRAD 3000
Online Services
SnagIt32
StartUp
< Back
Next >
Cancel

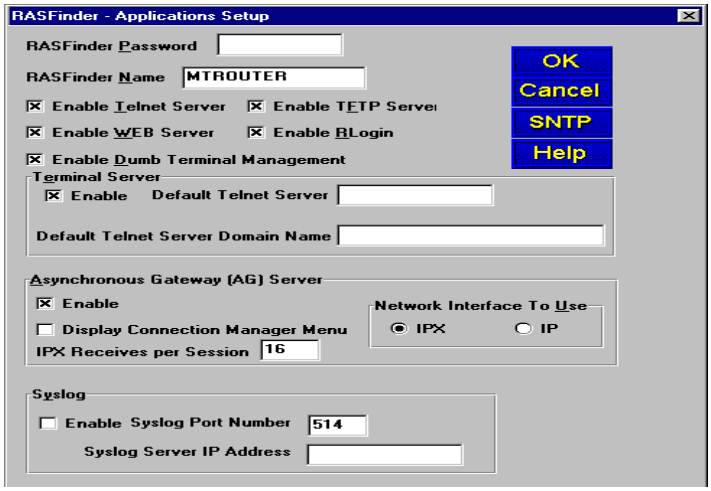
Click **Next** to accept the new folder designation, or choose an existing folder from the list provided.

8. The **Choose Network Type** screen displays.

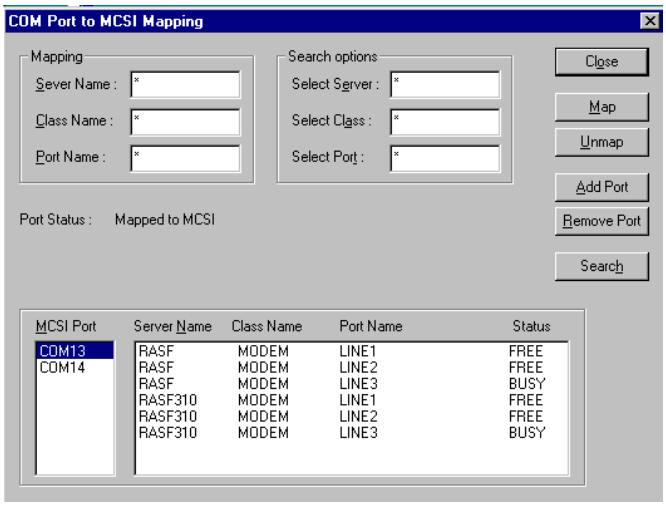


Selections include IPX, NetBIOS, and IP (default is IPX). Click **IP** and then click **Next** to proceed.

Note: If the software redirector is set up as IPX, the **IPX** option must be selected in the **Applications Setup** dialog box. If the software redirector is set up as IP, the **IP** option must be selected.



9. The **COM Port to MCSI Mapping** window displays.



Click **Add Port** to add a port to the **MCSI Port** list.

If you want a specific line, click a COM port in the **MCSI Port** list, then click the line to which you want to map that particular COM port. The status message "Mapped to MCSI" should appear above the **MCSI Port** list.

Click **Remove Port** to permanently remove a port from the **Local Port** list box.

Click **Unmap** to unmap a line.

Click **Search** to search for lines on a server.

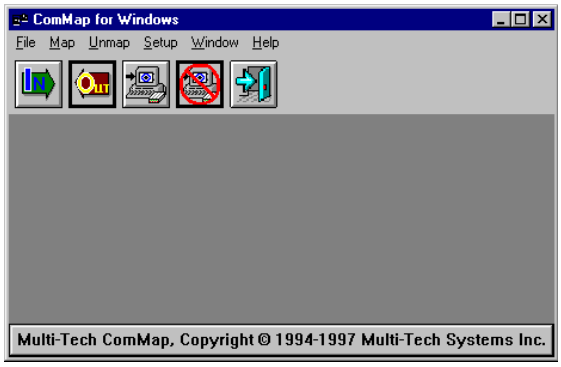
Click **Close** when finished.

At this time your WINMCSI software installation is complete. Proceed to the next section, “Running the WINMCSI Workstation Software”.

Running the WINMCSI Workstation Software

WINMCSI has a workstation portion of the software that LAN users run and use to log onto the communications server prior to running datacomm software on their client PCs. The following steps guide you through this process.

1. To start WINMCSI, click **Start** | **Programs** | **MultiTech MCSI** | **ComMap**. The **ComMap for Windows** window displays.



The buttons from left to right are: **Login**, **Logout**, **Map**, **Unmap**, and **Exit**.:

3. To setup **ComMap**, click **Setup**.

Click the **Network Type** command. The **Network Type** dialog box displays. Your current network type is highlighted. You can change the network type by clicking the option button appropriate for your network. Click **OK** when finished. You must restart Windows if you change this setting.

Note: Do not change the network type unless you have changed the network. Also, make sure that your SYSTEM.INI file contains the device drivers specific to the selected network type.

Click the **Connect Timer** command. The **MCSI Connect Timer** dialog box displays. The default value of the connect timer is shown in the Enter Connect Timer Value field. To change the value of the connect timer, type in a different value. Click **OK** when finished.

Click the **Baud Change** command. The **ComMap Baud Change** message displays. If baud change by an application is permitted, then this command is checked in the Setup Menu. If baud change is unchecked in the Setup Menu, then an application cannot change the baud rate (or other port parameters). Answer the message appropriately.

Click the **Default Login** command. The **Default Login Parameters** dialog box displays. Use this dialog box to select a specific RAS to which you want to log into next time Windows is loaded. Click a RAS from the **Available Servers** box. If there are no servers in the Available Servers box, then click the **Search** button. Type in a **User Name** and **Password** (optional) in their respective fields. Click **OK** when finished.

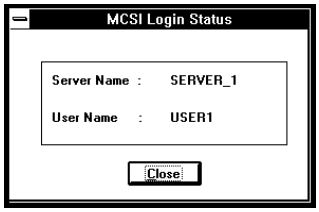
ComMap saves these login parameters in your COMMCSI.INI file.

Note: You cannot directly edit the COMMCSI.INI file using a text editor because the password field is encrypted.

4. If you have not logged into the network, do so now by clicking **File** | **Login**, or click **Login**. The **MCSI Login** window displays.

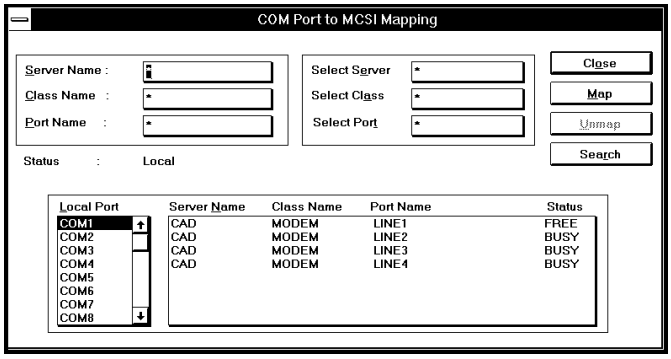
The **Available Servers** box lists the names of the available servers. Click the name of the server to which you want to attach, type a **User Name** and **Password** in their respective fields, and then click **Login**. A window displays stating that your login was successful. Click **OK**. If there are no servers listed in the **Available Servers** box, then click **Search** to search for a server.

5. At the **ComMap for Windows** main window, view your log status by clicking **File** | **Log Status**. The **MCSI Login Status** window displays.



This window shows the name of the server to which you are logged in and the name with which you logged in. Click **Close** when you are finished.

6. At the **ComMap for Windows** main window (to map a COM port through MCSI) click **Map** | **Map**. The **COM Port to MCSI Mapping** window displays.



Note: Windows 98/95 users will have two additional buttons in this box, the **Add Port** and the **Remove Port** buttons. You must click the **Add Port** button to view Local Ports. Click the **Remove Port** button to remove Local Ports.

If you want to get the first available line, click the **Map** button and then click the **Close** button and go to step 7.

If you want a specific line, click a COM Port in the Local Port list box, then click the line to which you want to map that particular COM Port. The status message "Mapped to MCSI" should appear above the Local Port list box.

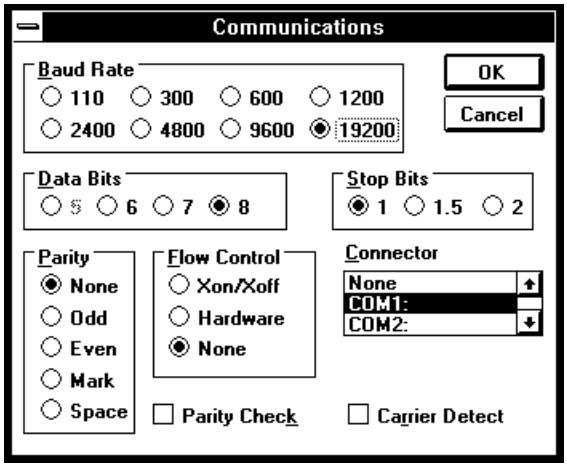
Click **Unmap** if you want to unmap a line.

Click **Search** to search for lines on a server.

Click **Close** when finished.

7. To view a list of mapped COM ports, click **Map** | **Map List**, or click the **Map** button. Click **Close** when finished.

   Below is an example of the Window's Terminal application's (shipped with all versions of Windows) **Communications** dialog box. After mapping your COM Ports with ComMap for Windows, you can check your connectivity and configure your ports with Windows Terminal. It is recommended that you use the settings shown in the example below (in the example COM1 is shown).



8. To unmap a COM port, click **Unmap** | **Unmap**, or click the **Unmap** button. Click the listing you want to unmap and then click **Unmap**.
9. To logout from the network, click **File** | **Logout**, or click the **Logout** button.
10. To exit from WINMCSI, click **File** | **Exit**, or click the **Exit** button. Otherwise you may minimize the screen to minimize WINMCSI to an icon.

RASFinder™
Remote Access Device

Chapter 6 - Remote Configuration and Management

MultiTech® Systems

Introduction

This chapter provides procedures for viewing or changing the configuration of a remote unit. Two methods are provided to access a remote unit; the first method is modem-based and the second method uses IP. Within the IP method, three different applications can be used: 1) LAN-Based configuration using TFTP (Trivial File Transfer Protocol), 2) Telnet as a client application, or 3) a standard Web browser on the Internet.

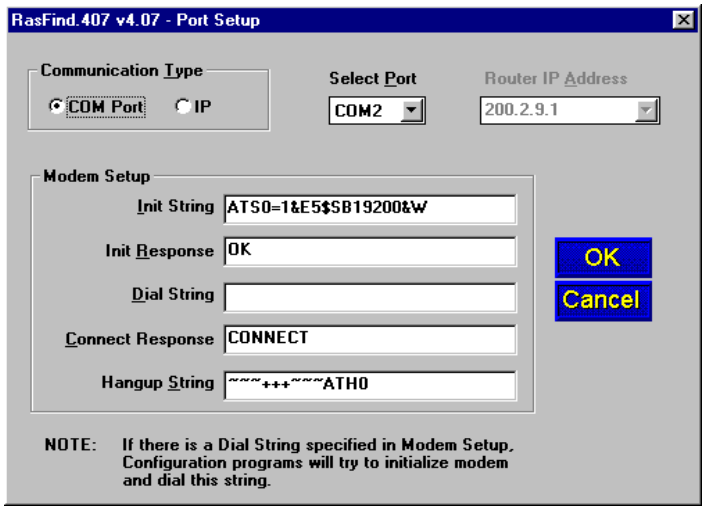
Remote Configuration

Remote configuration requires that the RASFinder software be installed on the local PC. The local PC then controls the remote RASFinder either through the modem connection or over the LAN.

Modem-Based

To remotely configure a RASFinder, a local PC needs to be connected to a dial-up line and the RASFinder software configured to call the remote RASFinder. The remote RASFinder needs to have a modem connected to a dial-up line and the Command port. Once the connection to the remote unit is made, you can change the configuration as required. Once the configuration is changed, you can download the new configuration to the remote RASFinder. Perform the following steps to remotely configure a RASFinder through a modem connection.

1. At the remote site, remove the serial cable from the PC to the Command port connector on the back panel of the RASFinder.
2. At the remote site, connect a special cable (Remote Configuration Cable) from the Command port connector on the back panel of the RASFinder to the RS-232 connector on the modem. The special cable is a serial cable with male connectors on both ends. Refer to Appendix A for cable details.
   a. Connect the modem to your local telephone line.
   b. Provide your telephone number to the person verifying your configuration.
   c. Configure the remote modem for 19200 baud and turn on Force DTR.
3. At the main site, connect your local PC to a modem that is connected to a dial-up line.
4. Install the RASFinder software on the local PC. When installed, click **Start** | **Programs** | **RASFinder** | **Configuration Port Setup**, or double-click the Configuration Port icon in the RASFinder program group.
5. The **Port Setup** dialog box displays.



Verify that the **Communication Type** field is set for **COM Port** and the **Select Port** option from the drop-down list matches the COM port of your local PC.

In the **Dial String** field, enter the AT command for dialing (ATDT) plus the phone number of the remote RASFinder.

If your Modem Initialization String, Initialization Response, or Connect Response values are different from the defaults in the dialog box, refer to your modem user documentation and change the values to match those required by your modem.

When you are satisfied with your selections, click **OK**.

6. Run the RASFinder Configuration program. Click **Start** | **Programs** | **RASFinder** | **RASFinder Configuration**, or double-click the RASFinder Configuration icon in the RASFinder program group.
7. The **Dialing Router** dialog box displays while software is dialing the remote RASFinder.
8. Once the **Dialing Router** dialog box completes, the **Reading Setup** dialog box displays.
9. Once the **Reading Setup** dialog box completes, the **RASFinder - Router Setup** dialog box displays. This is the remote RASFinder dialog box. Refer to the on-line Help for a description of each dialog box and field within a dialog box.

10. After you have changed the configuration of the remote RASFinder, click the **Download Setup** button to update the configuration. The remote RASFinder will be brought down, the new configuration written to the unit, and the unit will reboot.
11. After the downloading is complete, click **Exit**.
12. The **Hangup connection with Router?** dialog box displays

    Click **Yes** to disconnect the phone connection to the remote site.
13. If the same telephone number is not going to be used again in the immediate future, you may want to remove it from the **Port Setup** dialog box.
14. At the remote site, reconnect the RASFinder to the serial port of the PC and from the Program Manager screen click the **Router Configuration** Icon to verify that the RASFinder is running.

LAN-Based

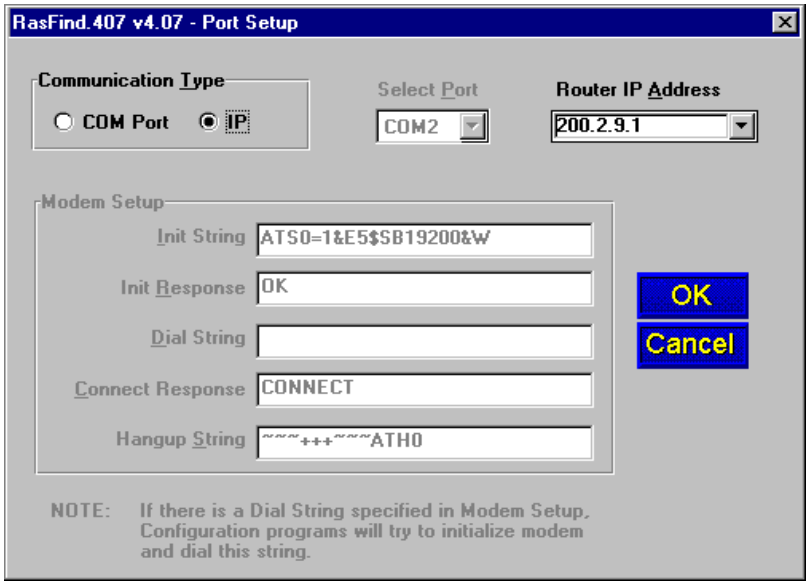
The LAN-based remote configuration requires a Windows Sockets compliant TCP/IP stack. TCP/IP protocol software must be installed and functional before the configuration program can be used.

1. You must assign an Internet (IP) address for the PC and for each node that will be managed by the configuration program. Refer to the protocol software documentation for instructions on how to set the IP addresses.

   Once you have completed this step, you should be able to use the protocol Ping command for the PC host name. You should also test the network interface configuration by Pinging another TCP/IP device that is connected to the network.

2. Install the RASFinder software on the local PC. When installed, click **Start** | **Programs** | **RASFinder** | **Configuration Port Setup**, or double-click the Configuration Port icon in the RASFinder program group.

3. The **Port Setup** dialog box displays.



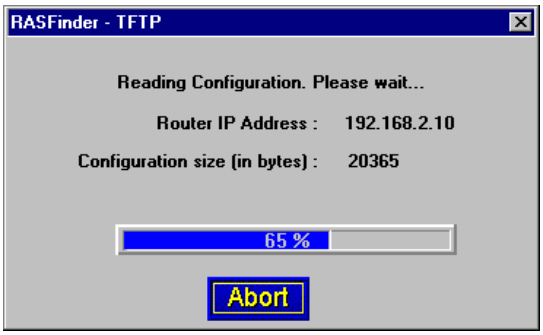
   Verify that the **Communication Type** field is set to **IP.**

   In the **Router IP Address** field, enter the IP Address of the remote RASFinder.

4. Click **OK** when you are satisfied with your selections.

5. Run the RASFinder Configuration program. Click **Start** | **Programs** | **RASFinder** | **RASFinder Configuration**, or double-click the RASFinder Configuration icon in the RASFinder program group.

   The following screen displays.



6. Once the program has completed reading the configuration, the **RASFinder - Router Setup** dialog box displays. This is the main menu for the *remote* RASFinder. Refer to the on-line Help for the definition of each dialog box and field within a dialog box.

7. After you have changed the configuration of the remote RASFinder, click **Download Setup** to update the configuration. The remote RASFinder will be brought down, the new configuration written to the unit, and the unit will reboot.

8. After downloading is complete, click **Exit**.

9. To verify that the RASFinder is running, double-click the **RASFinder Configuration** icon in the **RASFinder** program group.

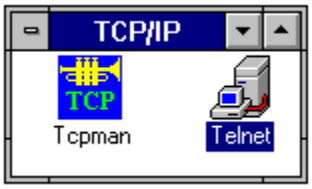
Remote Management

This section describes typical client applications that can be used to configure the RASFinder remotely. It is important to note that although any subsequent changes to configuration can be made using these methods, the initial setup and configuration of the RASFinder must be done from a local PC using the RASFinder software that is provided.

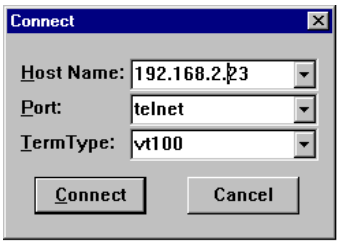
Although establishing access to the RASFinder varies between these applications, the configuration functions correspond to those of the RASFinder software run on a local PC. For more information on RASFinder software, refer to Chapter 4 - RASFinder Software.

Telnet

A typical Telnet client application is described next. The RASFinder has a built-in Telnet Server that enables Telnet client PCs to access the RASFinder. A typical Telnet client is allowed to configure the RASFinder and its data ports. In addition, the RASFinder can be remotely accessed and configured from anywhere on the connected Internet through its Web interface. A typical TCP/IP program group is shown below with a Tcpman icon and a Telnet icon.



The TCP/IP stack has to be loaded before the Telnet client (a Windows application) will run. The Telnet Server option has to be selected from the **Applications Setup** dialog box using the Router Configuration icon and the Others button on the **RASFinder - Router Setup** dialog box. Double-click the **Telnet** icon (or shortcut) and a blank Telnet screen displays. Click **Connect | Remote System** and the **Connect** dialog box displays. Select (or enter) a Host Name (the IP address of the RASFinder). In this example, the IP Host Name is 192.168.2.23.

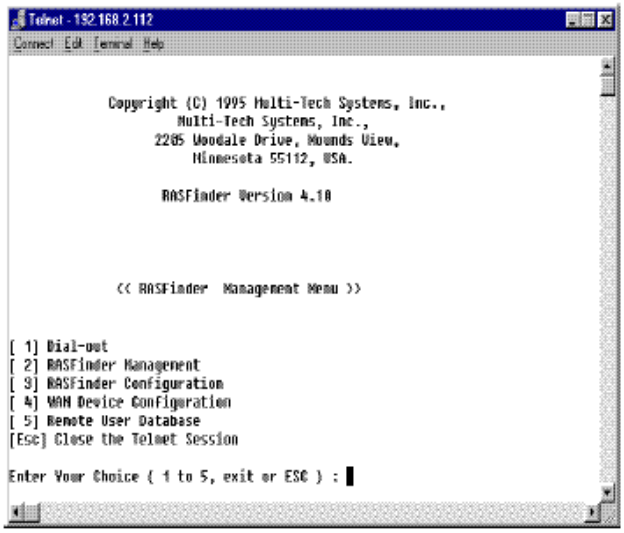


When you enter a valid Host Name (IP address) and click **Connect**, you are immediately connected to the target RASFinder and the RASFinder Management Menu screen displays.

RASFinder Management Menu

The RASFinder Management Menu provides five functional options in addition to the option of escaping and closing the Telnet session.

If you have entered a password in the **Applications Setup** dialog box in the RASFinder software, and have selected an option from the RASFinder Management Menu, you will need to enter your password before your choice is accepted.


Telnet - 192.168.2.112
Connect Edit Terminal Help
Copyright (C) 1995 Multi-Tech Systems, Inc.,
Multi-Tech Systems, Inc.,
2205 Woodale Drive, Mounds View,
Minnesota 55112, USA.
RASFinder Version 4.10
<< RASFinder Management Menu >>
[1] Dial-out
[2] RASFinder Management
[3] RASFinder Configuration
[4] WAN Device Configuration
[5] Remote User Database
[Esc] Close the Telnet Session
Enter Your Choice (1 to 5, exit or ESC) :

To select an option, enter the number of the option and hit the Enter key. For example, to select the Dial-Out option, type **1 <Enter>**. For details on a parameter, refer to the associated on-line Help.

Dial-Out

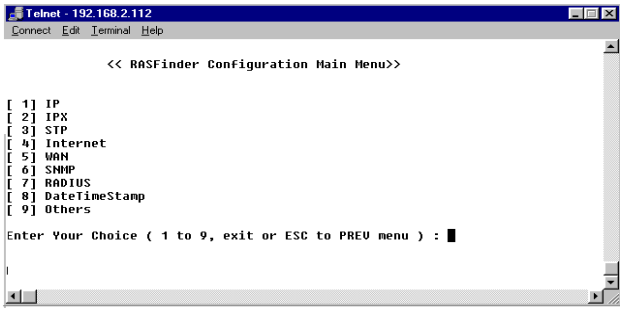
The Dial-out option (Option 1) on the RASFinder Management Menu enables a Telnet user to configure one of the WAN ports for a dial-out session. The default configuration of 115200 bps, 8N1 can be used for the dial-out session, or the user can specify each parameter for the port (e.g., the baud rate, the number of data bits, parity, or the number of stop bits). When the connection is established, anything entered on the keyboard is immediately presented to the selected WAN port. When the dial-out session is over, the WAN port reverts to its original configuration.

RASFinder Management

The RASFinder Management option (Option 2) on the RASFinder Management Menu enables a Telnet user to view router statistics or system information; another option enables the remote user to Reset the router.

RASFinder Configuration

The RASFinder Configuration option (Option 3) on the RASFinder Management Menu enables a Telnet user to view and change parameters on the protocol stacks, view or change bridge information, select PPP or SLIP, select a WAN port, or enable/disable the supported servers (applications).



WAN Device Configuration

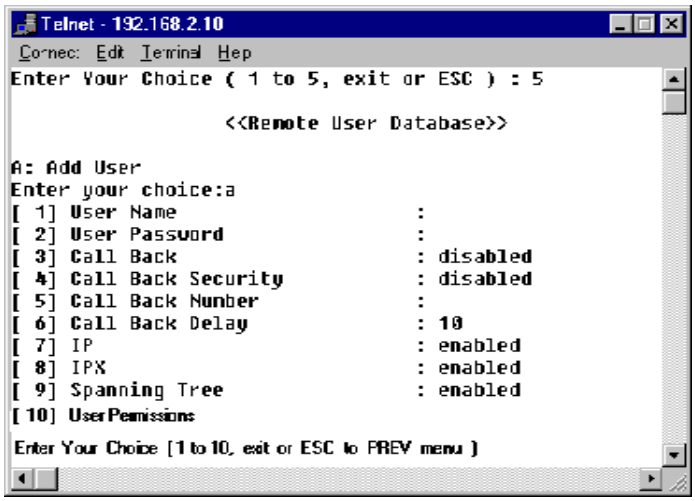
The WAN Device Configuration option (Option 4 on the RASFinder Management Menu) allows a remote user (a Telnet client) to put any port in WANTalk mode.

Remote User Database

The Remote User Database option (Option 5 on the RASFinder Management Menu) allows a remote user to add user information such as Name and Password, callback information, and which protocol stacks to enable or disable.

Remote User Database

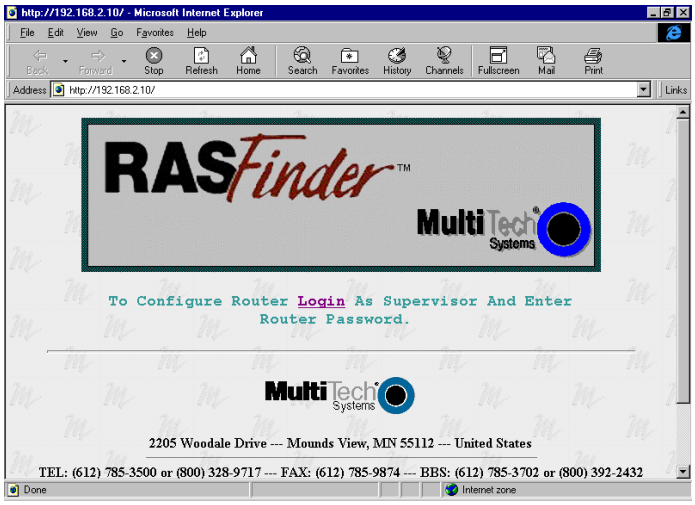
The Remote User Database option from the RASFinder Management Menu enables you to add and configure a list of users who will access the RASFinder remotely. After selecting Remote User Database (type **2 <Enter>**) from the main menu, type **A <Enter>** to add a new user to the database. The following list of options displays:


Telnet - 192.168.2.10
Connect Edit Terminal Help
Enter Your Choice (1 to 5, exit or ESC) : 5
<<Remote User Database>>
A: Add User
Enter your choice:a
[1] User Name :
[2] User Password :
[3] Call Back : disabled
[4] Call Back Security : disabled
[5] Call Back Number :
[6] Call Back Delay : 10
[7] IP : enabled
[8] IPX : enabled
[9] Spanning Tree : enabled
[10] User Permissions
Enter Your Choice [1 to 10, exit or ESC to PREV menu]

By selecting and configuring the various options and entering the desired information, you can construct a database of remote users for the RASFinder. For a detailed description of each option, refer to the on-line Help provided in your RASFinder software.

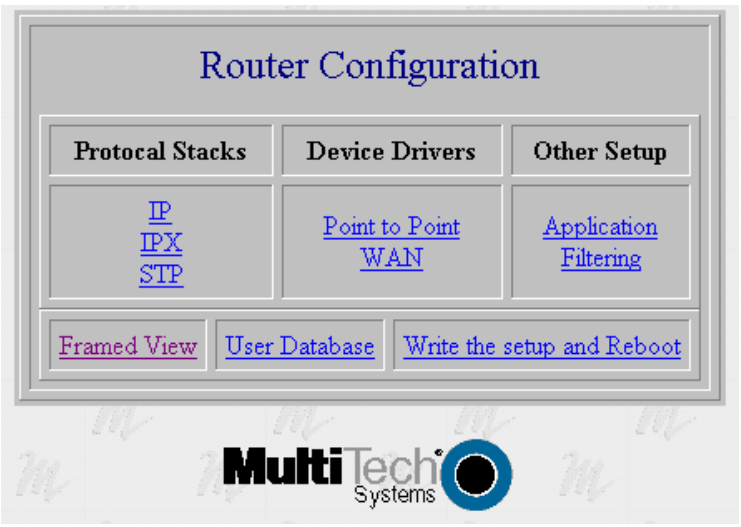
Web Browser Management

The RASFinder can be accessed, via a standard Web browser, from anywhere on the connected Internet. First, WEB Server must be checked (enabled) on the **Applications Setup** dialog box to enable this function. You can then access the **RASFinder Configuration** dialog box by typing the **IP Address** of the unit into the address line of your web browser. The following screen will be displayed:


http://192.168.2.10/ - Microsoft Internet Explorer
RASFinder
MultiTech Systems
To Configure Router Login As Supervisor And Enter Router Password.
2205 Woodale Drive --- Mounds View, MN 55112 --- United States
TEL: (612) 785-3500 or (800) 328-9717 --- FAX: (612) 785-9874 --- BBS: (612) 785-3702 or (800) 392-2432

Go to **Login** to gain access to the RASFinder. The following dialog box displays:

Type **supervisor** in the **User Name** box (no password is needed) and click **OK**.



Note: Only one user can access the RASFinder at any given time, and this user will have *read/write* rights over the unit.

RASFinder™
Remote Access Device

Chapter 7 - Service, Warranty and Tech Support

MultiTech® Systems

Limited Warranty

Multi-Tech Systems, Inc. (“MTS”) warrants that its products will be free from defects in material or workmanship for a period of two years from the date of purchase, or if proof of purchase is not provided, two years from date of shipment.

MTS MAKES NO OTHER WARRANTY, EXPRESSED OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED.

This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by the customer or any party without MTS’s written authorization, or used in any manner inconsistent with MTS’s instructions.

MTS’s entire obligation under this warranty shall be limited (at MTS’s option) to repair or replacement of any products which prove to be defective within the warranty period, or, at MTS’s option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS’s factory transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PURCHASE PRICE FOR DEFECTIVE PRODUCTS.

Repair Procedures for U.S. and Canadian Customers

In the event that service is required, products may be shipped, freight prepaid, to our Mounds View, Minnesota, factory:

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112
Attn: Repairs, Serial #_____

A Returned Materials Authorization (RMA) is not required. Return shipping charges (surface) will be paid by MTS to destinations in U.S. and Canada.

Please include inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), and your telephone number. If the product is out of warranty, a payment in advance is required. Acceptable means of payment include credit card, wire transfer or a check in U.S. dollars drawn on a U.S. Bank.

For out of warranty repair charges, go to COMPANY/Policies/warranty/

Extended two-year overnight replacement agreements are available for selected products. Please call MTS customer service at (888) 288-5470, or visit our web site at /PARTNERS/Programs/overnight_replacement/ for details on rates and coverages.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department at (800) 972-2439 or e-mail support@multitech.com. Please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at (800) 328-9717 or (763) 717-5631, or e-mail mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Customers

(outside U.S.A. and Canada)

Your original point of purchase reseller may offer the quickest and most economical repair option for your Multi-Tech product. You may also contact any Multi-Tech sales office for information about the nearest distributor or other repair service for your Multi-Tech product at www.multitech.com/PARTNERS/channels/offices/.

In the event that factory service is required, products may be shipped, freight prepaid, to our Mounds View, Minnesota, factory. Recommended international shipment methods are via Federal Express, UPS or DHL courier services, or by airmail parcel post; shipments made by any other method will be refused. Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), and your telephone number. If the product is out of warranty, a payment in advance is required. Acceptable means of payment include credit card, wire transfer or a check drawn on a U.S. bank. Repaired units will be shipped freight collect, unless other arrangements are made in advance.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department nearest you, or e-mail support@multitech.com. When calling the U.S., please direct questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at +(763) 717-5631 in the U.S.A., or e-mail mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Distributors

International distributors should contact their MTS International sales representative for information about the repair of Multi-Tech product(s).

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our International Technical Support department +(763) 717-5863. When calling the U.S., please direct questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at +(763) 717-5631 in the U.S.A., or e-mail mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Replacement Parts

SupplyNet, Inc., can supply you with replacement power supplies, cables and connectors for selected Multi-Tech products. You can place an order with SupplyNet via mail, phone, fax or the Internet at the following addresses:

Mail: SupplyNet, Inc.
614 Corporate Way
Valley Cottage, NY 10989
Phone: 800 826-0279
Fax: 914 267-2420
Email: *info@thesupplynet.com*
Internet: *http://www.thesupplynet.com*

Technical Support

Multi-Tech Systems has an excellent staff of technical support personnel available to help you get the most out of your Multi-Tech product. If you have any questions about the operation of this unit, please call 800 972-2439 (USA and Canada) or 763 785-3500 (international and local). Please have product information available. You can also contact Technical Support by e-mail at the following addresses:

Country	Email	Telephone
France:	support@multitech.fr	+(33) 1-64 61 09 81
Europe, Asia, Africa.:	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others;	support@multitech.com	800-972-2439 or 763-717-5863

Please note the status of the product before contacting Technical Support. Status information can include the state of the LED indicators, screen messages, diagnostic test results, problems with a specific application, etc.

Internet Sites

Multi-Tech is a commercial provider on the Internet. Multi-Tech has a Web site at http://www.multitech.com

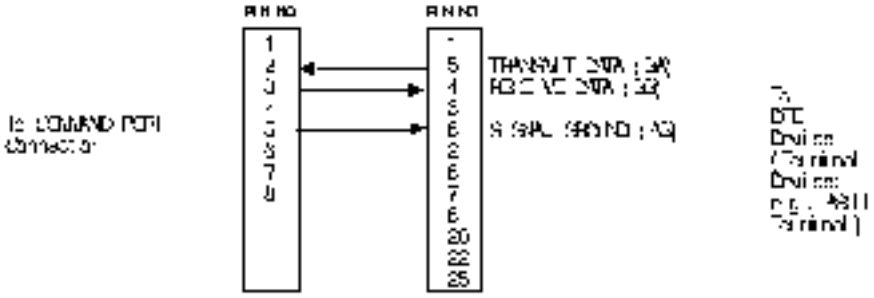
RASFinder™
Remote Access Device

Appendixes

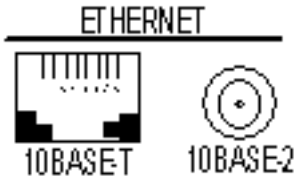
MultiTech® Systems

Appendix A - Cabling Diagrams

Command Port Cable

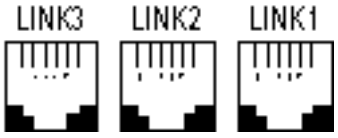


LAN Cables



Pin	Circuit Signal Name	Pin	Description
1	TD+ Data Transmit Positive	1	Center
2	TD- Data Transmit Negative	2	Shield
3	RD+ Data Receive Positive		
6	RD- Data Receive Negative		

WAN Cables



Pin	Circuit
3	Tip
4	Ring

Appendix B - Script Language

A script file can be used to automate certain operations. The script file is a text file containing a sequence of the following commands (listed here according to their functions). This is similar to what you will find in the Help file in your ProxyServer software. Following the list of commands is an example script.

Commands (by Function)

Dial, Connection and Remote

ACTIVATEDOD	BAUDRATE	BREAK
GETCTS	GETDCD	HANGUP
PARITYR	GETC	RGETS
RXFLUSH	SETDTR	SETRTS
STOPBITS	THISLAYERUP	TRANSMIT
TXFLUSH	WAITFOR	

Mathematical functions

DEC	INC

Miscellaneous

EXIT	WAIT

Program constructs

FOR	IF	PROC
SWITCH	WHILE	

String operations

ATOI	ITOA	STRCAT
STRCMP	STRCOPY	STRFMT
STRLEN	TOLOWER	TOUPPER

Example Script:

```
proc main;
      string login_prompt;
      string user_name;
      string password_prompt;
      string password;
      string shell_menu;
      string shell_menu_response;
      integer timeout;

      timeout=10;
      login_prompt=”login:”;
      user_name=”user1”;
      password_prompt=”Password:”;
      password=”user1”;
      shell_menu=”choice:”;
      shell_menu_response=”1”;

      transmit(“A”);
      wait(1)
      transmit(“T^M”);
      waitfor (“OK”,10);

      transmit (“A”);
      wait (1);
      transmit (“T”);
      wait (1);
      transmit (“DT963^M”);

      if (waitfor (login_prompt,60))  then
          transmit (user_name);
          transmit (“^M”);
          if (waitfor (password_prompt,timeout))  then
                transmit (password);
                transmit (“^M”);
                 if (waitfor (shell_menu,timeout))  then
                        transmit (shell_menu_response);
                       transmit (“^M”);
        else
                        transmit (“Shell Menu Not Received^M”);
        endif
      else
        transmit (“Password Prompt Not Received^M”);
        endif
      else
        transmit (“Login Prompt Not Received^M”);
      endif


Endproc
```

Appendix C - Regulatory Information

Class B Statement

FCC Part 15

NOTE: This equipment has been tested and found to comply with the limits for a **Class B** digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

Fax Branding Statement

The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device, including fax machines, to send any message unless such message clearly contains the following information:

- Date and time the message is sent
- Identification of the business or other entity, or other individual sending the message
- Phone number of the sending machine or such business, other entity, or individual

This information is to appear in a margin at the top or bottom of each transmitted page or on the first page of the transmission. (Adding this information in the margin is referred to as *fax branding*.)

Since any number of Fax software packages can be used with this product, the user must refer to the Fax software manual for setup details. Typically, the Fax branding information must be entered via the configuration menu of the software.

FCC Part 68 Telecom

1. This equipment complies with Part 68 of the Federal Communications Commission (FCC) rules. On the outside surface of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN). If requested, this information must be provided to the telephone company.
2. As indicated below, the suitable jack (Universal Service Order Code connecting arrangement) for this equipment is shown. If applicable, the facility interface codes (FIC) and service order codes (SOC) are shown. An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68 compliant. See installation instructions for details.
3. The ringer equivalence number (REN) is used to determine the number of devices which may be connected to the telephone line. Excessive REN's on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total REN's, contact the telephone company to determine the maximum REN for the calling area.
4. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
5. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications in order to maintain uninterrupted service.
6. If trouble is experienced with this equipment (the model of which is indicated below) please contact Multi-Tech Systems, Inc., at the address shown below for details of how to have repairs made. If the equipment is causing harm to the telephone network, the telephone company may request that you remove the equipment from the network until the problem is resolved.
7. No repairs are to be made by you. Repairs are to be made only by Multi-Tech Systems or its licensees. Unauthorized repairs void registration and warranty.
8. This equipment cannot be used on public coin service provided by the telephone company. Connection to Party Line Service is subject to state tariffs. (Contact the state public utility commission, public service commission or corporation commission for information.)
9. If so required, this equipment is hearing-aid compatible.

Manufacturer:	Multi-Tech Systems, Inc.
Trade name:	RASFinder
Model Numbers:	MTASR3-200
FCC Registration Number:	AU7USA-24994-M5-E
Ringer Equivalence:	0.6B
Modular Jack:	RJ-11C or RJ-11W
Service Center in U.S.A.:	Multi-Tech Systems Inc. 2205 Woodale Drive Mounds View, MN 55112 (763) 785-3500 Fax (763) 785-9874

Canadian Limitations Notice

Ringer Equivalence Number

Notice: The ringer equivalence number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a phone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the ringer equivalence numbers of all the devices does not exceed 5.

Notice: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, phone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

CE

EMC, Safety and Terminal Directive Compliance

The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility.

and

Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits:

and

Council Directive 98/13/EC of 12 March 1998 on the approximation of the laws of Member States concerning telecommunications terminal and Satellite earth station equipment.

Appendix D - AT Command Summary

This Appendix summarizes the AT commands for the RASFinder modems.

Command: **+++AT<CR> Escape Sequence**
Values: n/a
Description: Puts the modem in command mode (and optionally issues a command) while remaining on-line. Type **+++AT** and up to ten command characters, then press ENTER. Used mostly to issue the hang-up command: **+++ATH<CR>**.

Command: **AT Attention Code**
Values: n/a
Description: The attention code precedes all command lines except **A/** and the escape sequence.

Command: **ENTER Key**
Values: n/a
Description: Press the ENTER key to execute most commands.

Command: **$ Detect AT&T's "call card" tone**
Values: n/a
Description: This symbol placed in dialing string enables the modem to detect AT&T's "call card" tones to access user's calling card when originating an on-line connection--

ATDT1028806127853500$123456789
(access/phone number) (Credit Card number)

Command: **A Answer**
Values: n/a
Description: Answer an incoming call before the final ring.

Command: **A/ Repeat Last Command**
Values: n/a
Description: Repeat the last command string. Do not precede this command with **AT**. Do not press ENTER to execute.

Command: **B*n* Communication Standard Setting**
Values: *n* = 0–3, 15, 16
Default: 1 and 16
Description:
- B0 Select ITU-T V.22 mode when modem is at 1200 bps.
- B1 Select Bell 212A when modem is at 1200 bps.
- B2 Deselect V.23 reverse channel (same as B3).
- B3 Deselect V.23 reverse channel (same as B2).
- B15 Select V.21 when the modem is at 300 bps.
- B16 Select Bell 103J when the modem is at 300 bps.

Command: **C*n* Carrier Control**
Values: *n* = 1
Default: 1
Description:
- C0 Transmit carrier always off. (Not supported.)
- C1 Normal transmit carrier switching (included for backward compatibility with some software).

Command: **D*s*** **Dial**
Values: *s* = dial string (phone number and dial modifiers)
Default: none
Description: Dial phone number *s*, where *s* may up to 40 characters long and include the 0–9, *, #, A, B, C, and D characters, and the **L**, **P**, **T**, **V**, **W**, **S**, comma (**,**), semicolon (**;**), **!**, @, **^** and **$** dial string modifiers.

Dial string modifiers:

L Redial last number. (Must be placed immediately after **ATD**.)
P Pulse-dial following numbers in command .
T Tone-dial following numbers in command (default).
V Switch to speakerphone mode and dial the following number. Use **ATH** command to hang up.
W Wait for a new dial tone before continuing to dial. (**X2**, **X4**, **X5**, **X6**, or **X7** must be selected.)
S Dial a phone number previously stored using the &Zn=x command (see &Zn=x command for further information). The range of n is 0-3.
, Pause during dialing for time set in register S8.
; Return to command mode after dialing. (Place at end of dial string.)
! Hook flash. Causes the modem to go on-hook for one-half second, then off-hook again.
@ Wait for quiet answer. Causes modem to wait for a ringback, then 5 seconds of silence, before processing next part of command. If silence is not detected, the modem returns a NO ANSWER code.
$ AT&T's "call card" tones detection.
^ Disable data calling tone transmission.

Command: **DS=*n*** **Dial Stored Telephone Number**
Values: *n* = 0–3
Default: none
Description: Dial a number previously stored in directory number *n* by the ***&Zn=x*** command .
Example: **ATDS=3**

Command: **E*n*** **Echo Command Mode Characters**
Values: *n* = 0 or 1
Default: 1
Description: E0 Do not echo keyboard input to the terminal.
E1 Do echo keyboard input to the terminal.

Command: **F*n*** **Echo Online Data Characters**
Values: *n* = 1
Default: 1
Description: F0 Enable on-line data character echo. (Not supported.)
F1 Disable on-line data character echo (included for backward compatibility with some software).

Command: **H*n*** **Hook Control**
Values: *n* = 0 or 1
Default: 0
Description: H0 Go on-hook to hang up.
H1 Go off-hook to make the phone line busy.

Command: **I*n*** **Information Request**
Values: *n* = 0–4, 9, 11
Default: None
Description: I0 Display default speed and controller firmware version.
I1 Calculate and display ROM checksum (e.g., “12AB”).
I2 Check ROM and verify the checksum, displaying *OK* or *ERROR*.
I3 Display default speed and controller firmware version.
I4 Display firmware version for data pump (e.g., “94”).
I9 Display country code (e.g., “NA Ver. 1”).
I11 Display Diagnostic Information for the last Modem Connection (i.e., DSP and Firmware version, Link Type, Line Speed, Serial Speed, Type of Error Correction/Data Compression, Number of past Retrains,etc.)

Command:	**L*n***	**Monitor Speaker Volume**
Values:		*n* = 0, 1, 2, or 3
Default:		2
Description:	L0	Select low volume.
	L1	Select low volume.
	L2	Select medium volume.
	L3	Select high volume.

Command:	**M*n***	**Monitor Speaker Mode**
Values:		*n* = 0, 1, 2, or 3
Default:		1
Description:	M0	Speaker always off.
	M1	Speaker on until carrier signal detected.
	M2	Speaker always on when modem is off-hook.
	M3	Speaker on until carrier is detected, except while dialing.

Command:	**N*n***	**Modulation Handshake**
Values:		*n* = 0 or 1
Default:		1
Description:	N0	Modem performs handshake only at communication standard specified by S37 and the ***B*** command.
	N1	Modem begins handshake at communication standard specified by S37 and the ***B*** command. During handshake, fallback to a lower speed can occur.

Command:	**O**	**Return Online to Data Mode**
Values:		0, 1, 3
Default:		None
Description:	O0	Exit on-line command mode and return to data mode.
	O1	Issue a retrain and return to on-line data mode.
	O3	Issue a rate renegotiation and return to data mode.

Command:	**Q*n***	**Result Codes Enable/Disable**
Values:		*n* = 0 or 1
Default:		0
Description:	Q0	Enable result codes.
	Q1	Disable result codes.

Command:	**S*r*=*n***	**Set Register Value**
Values:		*r* = S-register number; *n* varies
Default:		None
Description:		Set value of register S*r* to value of *n*, where *n* is entered in decimal format.

Command:	**S*r*?**	**Read Register Value**
Values:		*r* = S-register number
Default:		None
Description:		Read value of register S*r* and display value in 3-digit decimal form.

Command:	**V*n***	**Result Code Format**
Values:		*n* = 0 or 1
Default:		1
Description:	V0	Displays result codes as digits (terse response).
	V1	Displays result codes as words (verbose response).

Command:	**X*n***	**Result Code Selection**
Values:		*n* = 0–7
Default:		4
Description:	X0	Basic result codes (*e.g., CONNECT*); does not look for dial tone or busy signal.
	X1	Extended result codes (*CONNECT 56000 V42bis, CONNECT 33600 V42bis*, etc.); does not look for dial tone or busy signal.
	X2	Extended result codes with *NO DIALTONE*; does not look for busy signal.
	X3	Extended result codes with *BUSY*; does not look for dial tone.
	X4	Extended result codes with *NO DIALTONE* and *BUSY*.

	X5	Extended result codes with *NO DIALTONE* and *BUSY*.
	X6	Extended result codes with *NO DIALTONE* and *BUSY*.
	X7	Basic result codes with *NO DIALTONE* and *BUSY*.

Command: **Y*n*** **Long Space Disconnect**
Values: *n* = 0
Default: 0
Description:
- Y0 Disable sending or responding to long space break signal on disconnect.
- Y1 Enable sending or responding to long space break signal on disconnect. (Not supported.)

Command: **Z*n*** **Modem Reset**
Values: *n* = 0 or 1
Default: None
Description:
- Z0 Reset modem to profile saved by the last ***&W*** command.
- Z1 Same as Z0.

Command: **&B*n*** **V.32 Auto Retrain**
Values: *n* = 1
Default: 1
Description:
- &B0 Disable V.32 auto retrain. (Not supported.)
- &B1 Enable V.32 auto retrain.

Command: **&C*n*** **Data Carrier Detect (DCD) Control**
Values: *n* = 0 or 1
Default: 1
Description:
- &C0 Force Data Carrier Detect signal high.
- &C1 Let Data Carrier Detect follow carrier signal.

Command: **&D*n*** **Data Terminal Ready (DTR) Control**
Values: *n* = 0, 1, 2, or 3
Default: 2
Description:
- &D0 Modem ignores DTR signal.
- &D1 When DTR drops while in on-line data mode, the modem enters command mode, issues an OK, and remains connected.
- &D2 When DTR drops while in on-line data mode, the modem hangs up.
- &D3 When DTR drops, the modem hangs up and resets as if an **ATZ** command were issued.

Command: **&F*n*** **Load Factory Default Settings**
Values: *n* = 0
Default: None
Description:
- &F0 Load factory settings as active configuration.

Command: **&G*n*** **V.22bis Guard Tone Control**
Values: *n* = 0, 1, or 2
Default: 0
Description:
- &G0 Disable guard tone.
- &G1 Enable 550 Hz guard tone.
- &G2 Enable 1800 Hz guard tone.

✉: The ***&G*** command is not used in North America.

Command: **&J*n*** **Auxiliary Relay Control**
Values: *n* = 0
Default: 0
Description:
- &J0 The auxiliary relay is never closed.
- &J1 Not supported—responds ERROR.

Command: **&K*n*** **Local Flow Control Selection**
Values: *n* = 0, 3, or 4
Defaults: 3
Description: &K0 Flow control disabled.
&K3 Enable CTS/RTS hardware flow control.
&K4 Enable XON/XOFF software flow control.

Command: **&M*n*** **Communications Mode**
Values: *n* = 0
Defaults: 0
Description: &M0 Asynchronous mode.
&M1 Reserved—responds ERROR.

Command: **&Q*n*** **Asynchronous Communications Mode**
Values: *n* = 0, 5, or 6
Defaults: 5
Description: &Q0 Asynchronous with data buffering. Same as ***I0***.
&Q5 Error control with data buffering. Same as ***I3***.
&Q6 Asynchronous with data buffering. Same as ***I0***.

Command: **&S*n*** **Data Set Ready (DSR) Control**
Values: *n* = 0 or 1
Default: 0
Description: &S0 Force DSR high (on).
&S1 Let DSR follow CD.

Command: **&T*n*** **Self-Test Commands**
Values: *n* = 0, 1, 3 or 6
Default: None
Description: &T0 Abort. Stop any test in progress.
&T1 Local analog loop test.
&T3 Local digital loopback test.
&T6 Remote digital loopback test.

Command: **&V** **View Current Configuration**
Values: n/a
Description: Displays the active modem settings.

Command: **&W*n*** **Store Current Configuration**
Values: *n* = 0
Default: None
Description: &W0 Store active modem settings in NVRAM; load them at power-on or following the **ATZ** command instead of loading the factory defaults from ROM.

Command: **&Y*n*** **Select Stored Configuration for Hard Reset**
Values: *n* = 0
Default: 0
Description: &Y0 Select stored configuration 0 on power-up. (For backward compatibility with some software.)
&Y1 Not supported—responds ERROR.

Command: **&Z*n*=*x*** **Store Telephone Number**
Values: *n* = 0, 1, 2, or 3
x = Dialing string
Default: None
Description: Stores telephone dial string *x* in memory location *n*. Dial the stored number using the command ***ATDS=n***.

Command: **\G*n*** **Modem Port Flow Control**
Values: *n* = 0
Default: 0
Description: \G0 Returns an *OK* for backward compatibility with some software.
\G1 Not supported—responds ERROR.

Command: **\J*n*** **Data Buffer Control**
Values: *n* = 0
Default: 0
Description: \J0 Enable data buffer—serial port speed is independent of connect speed.
\J1 Not supported—responds ERROR.

Command: **\K*n*** **Set Break Control**
Values: *n* = 5
Default: 5
Description: \K5 Modem sends break signal received from the DTE to the remote modem.

Command: **\N*n*** **Error Correction Mode Selection**
Values: *n* = 0–5, or 7
Default: 3
Description: \N0 Non-error correction mode with data buffering (same as ***&Q6***).
\N1 Direct mode.
\N2 MNP reliable mode.
\N3 V.42/MNP auto-reliable mode.
\N4 V.42 reliable mode.
\N5 V.42, MNP, or non-error correction (same as ***\N3***).
\N7 V.42, MNP, or non-error correction (same as ***\N3***).

Command: **\Q*n*** **Local Flow Control Selection**
Values: *n* = 0, 1, or 3
Default: 3
Description: \Q0 Disable flow control (same as ***&K0***).
\Q1 XON/XOFF software flow control (same as ***&K4***).
\Q2 CTS-only flow control. Not supported—responds ERROR.
\Q3 RTS/CTS hardware flow control (same as ***&K3***).

Command: **\T*n*** **Inactivity Timer**
Values: *n* = 0–255
Default: n/a
Description: \Tn Inactivity timer setting contingent on either \T value or S-Register S30 value (e.g., AT\T45&W0<cr> configures in parallel ATS30=45&W0<cr>), and vice versa.

Command: **\V*n*** **Protocol Result Code**
Values: *n* = 0 or 1
Default: 1
Description: \V0 Disable protocol result code appended to DCE speed.
\V1 Enable protocol result code appended to DCE speed.

Command: **\X*n*** **XON/XOFF Pass-Through**
Values: *n* = 0 or 1
Defaults: 0
Description: \X0 Respond to and discard XON/XOFF characters.
\X1 Not supported—responds ERROR.

Command: **-C*n*** **Data Calling Tone**
Values: *n* = 0 or 1
Defaults: 0
Description: -C0 Disable V.25 data calling tone.
-C1 Enable V.25 data calling tone.

Command: **%B** **View Numbers in Blacklist**
Values: n/a
Description: If blacklisting is in effect, this command displays the numbers for which the last call attempted in the previous two hours failed. In countries that do not require blacklisting, the ERROR result code appears.

Command: **%C*n*** **Data Compression Control**
Values: *n* = 0 or 1
Default: 1
Description: %C0 Disable V.42bis/MNP 5 data compression.
%C1 Enable V.42bis/MNP 5 data compression.

Command: **+ES=6** **Enable Synchronous Buffered Mode**
Values: n/a
Description: Allows an H.324 video application direct access to the synchronous data channel. On underflow, the modem sends HDLC flag idle (0x7E) to the remote modem. This special error correction mode is overridden by any of the following commands: ***&F***, ***&M***, ***&Q***, and ***\N***. ***+ES = ?*** shows the only allowed value.

Command: **&&S** **Speaker Codec Loopback**
Values: n/a
Description: Provides a loopback from the microphone to the speaker. *For testing and debugging only.*

Command: **%T94** **Testing External RAM**
Values: n/a
Description: This command is used for testing the external RAM. Enter AT%T94<cr> to determine the status of external RAM. The response you should receive will be either "FAIL" or "PASS"

Command: **%T125** **Testing DSP 56K Code Version/Checksum**
Values: n/a
Description: Entering AT%T125<cr> tests the DSP56K code version and checksum running in external RAM. Upon issuing this command the user may then issue ATI4<cr> to get DSP version or ATI1<cr> to get DSP checksum in RAM.
Entering AT%T124<cr> tests the DSP56K code version and checksum running in internal ROM. Upon issuing this command the user may then issue ATI4<cr> to get DSP version or ATI1<cr> to get DSP checksum in ROM.

Appendix E - TCP/IP

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a protocol suite and related applications developed for the U.S. Department of Defense in the 1970s and 1980s specifically to permit different types of computers to communicate and exchange information with one another. TCP/IP is currently mandated as an official U.S. Department of Defense protocol and is also widely used in the UNIX community.

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. First, choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You'll need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses.

Early IP implementations ran on hosts commonly interconnected by Ethernet local area networks (LAN). Every transmission on the LAN contains the local network, or medium access control (MAC), address of the source and destination nodes. The MAC address is 48-bits in length and is non-hierarchical; MAC addresses are never the same as IP addresses.

When a host needs to send a datagram to another host on the same network, the sending application must know both the IP and MAC addresses of the intended receiver. Unfortunately, the IP process may not know the MAC address of the receiver. The Address Resolution Protocol (ARP), described in RFC 826 (located at ftp://ds.internic.net/rfc/rfc826.txt) provides a mechanism for a host to determine a receiver's MAC address from the IP address. In the process, the host sends an ARP packet in a frame containing the MAC broadcast address; and then the ARP request advertises the destination IP address and asks for the associated MAC address. The station on the LAN that recognizes its own IP address will send an ARP response with its own MAC address. An ARP message is carried directly in an IP datagram.

Other address resolution procedures have also been defined, including those which allow a diskless processor to determine its IP address from its MAC address (Reverse ARP, or RARP), provides a mapping between an IP address and a frame relay virtual circuit identifier (Inverse ARP, or InARP), and provides a mapping between an IP address and ATM virtual path/channel identifiers (ATMARP).

The TCP/IP protocol suite comprises two protocols that correspond roughly to the OSI Transport and Session Layers; these protocols are called the Transmission Control Protocol and the User Datagram Protocol (UDP). Individual applications are referred to by a port identifier in TCP/UDP messages. The port identifier and IP address together form a "socket". Well-known port numbers on the server side of a connection include 20 (FTP data transfer), 21 (FTP control), 23 (Telnet), 25 (SMTP), 43 (whois), 70 (Gopher), 79 (finger), and 80 (HTTP).

TCP, described in RFC 793 (ftp://ds.internic.net/rfc/rfc793.txt) provides a virtual circuit (connection-oriented) communication service across the network. TCP includes rules for formatting messages, establishing and terminating virtual circuits, sequencing, flow control, and error correction. Most of the applications in the TCP/IP suite operate over the "reliable" transport service provided by TCP.

UDP, described in RFC 768 (ftp://ds.internic.net/rfc/rfc768.txt) provides an end-to-end datagram

(connectionless) service. Some applications, such as those that involve a simple query and response, are better suited to the datagram service of UDP because there is no time lost to virtual circuit establishment and termination. UDP's primary function is to add a port number to the IP address to provide a socket for the application.

The Application Layer protocols are examples of common TCP/IP applications and utilities, which include:

- Telnet (Telecommunication Network): a virtual terminal protocol allowing a user logged on to one TCP/IP host to access other hosts on the network, described in RFC 854 (ftp://ds.internic.net/rfc/rfc854.txt).
- FTP: the File Transfer Protocol allows a user to transfer files between local and remote host computers per IETF RFC 959 (ftp://ds.internic.net/rfc/rfc959.txt).
- Archie: a utility that allows a user to search all registered anonymous FTP sites for files on a specified topic.
- Gopher: a tool that allows users to search through data repositories using a menu-driven, hierarchical interface, with links to other sites, per RFC 1436 (ftp://ds.internic.net/rfc/rfc1436.txt).
- SMTP: the Simple Mail Transfer Protocol is the standard protocol for the exchange of electronic mail over the Internet, per IETF RFC 821 (ftp://ds.internic.net/rfc/rfc821.txt).
- HTTP: the Hypertext Transfer Protocol is the basis for exchange of information over the World Wide Web (WWW). Various versions of HTTP are in use over the Internet, with HTTP version 1.0 (per RFC 1945) (ftp://ds.internic.net/rfc/rfc1945.txt) being the most current.
- HTML: WWW pages are written in the Hypertext Markup Language (HTML), an ASCII-based, platform-independent formatting language, per IETF RFC 1866 (ftp://ds.internic.net/rfc/rfc1866.txt).
- Finger: used to determine the status of other hosts and/or users, per IETF RFC 1288 (ftp://ds.internic.net/rfc/rfc1288.txt).
- POP: the Post Office Protocol defines a simple interface between a user's mail reader software and an electronic mail server; the current version is POP3, described in IETF RFC 1460 (ftp://ds.internic.net/rfc/rfc1460.txt).
- DNS: the Domain Name System defines the structure of Internet names and their association with IP addresses, as well as the association of mail, name, and other servers with domains.
- SNMP: the Simple Network Management Protocol defines procedures and management information databases for managing TCP/IP-based network devices. SNMP, defined by RFC 1157 (ftp://ds.internic.net/rfc/rfc1157.txt) is widely deployed in local and wide area network. SNMP Version 2 (SNMPv2), per RFC 1441< ftp://ds.internic.net/rfc/rfc1441.txt) adds security mechanisms that are missing in SNMP, but is also more complex.
- Ping: a utility that allows a user at one system to determine the status of other hosts and the latency in getting a message to that host. Ping uses ICMP Echo messages.
- Whois/NICNAME: Utilities that search databases for information about Internet domain and domain contact information, per RFC 954 (ftp://ds.internic.net/rfc/rfc954.txt).
- Traceroute: a tool that displays the route that packets will take when traveling to a remote host.

Internet Protocol (IP)

IP is the Internet standard protocol that tracks Internetwork node addresses, routes outgoing messages and recognizes incoming messages, allowing a message to cross multiple networks on the way to its final destination. The IPv6 Control Protocol (IPV6CP) is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. IPV6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPV6CP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. IPV6CP packets received before this phase is reached are silently discarded. (See also TCP/IP.)

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. You first choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations, etc.). Next, you determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses. The current demand for Internet connections will exhaust the current stock of 32-bit IP addresses. In response, Internet architects have proposed the next generation of IP addresses, IPng (IP Next Generation). It will feature 16-byte (128-bit) addressing, surpassing the capacities of 32-bit IP. Still in its design phase, IPng (also known as IPv6) is not expected to be widely deployed before the end of this century.

An IP address can serve only a single physical network. Therefore, if your organization has multiple physical networks, you must make them appear as one to external users. This is done via "subnetting", a complex procedure best left to ISPs and others experienced in IP addressing. Since IP addresses and domain names have no inherent connection, they are mapped together in databases stored on Domain Name Servers (DNS). If you decide to let an Internet Service Provider (ISP) administer your DNS server, the ISP can assist you with the domain name and IP address assignment necessary to configure your company's site-specific system information. Domain names and IP addresses are granted by the InterNIC. To check the availability of a specific name or to obtain more information, call the InterNIC at (703)742-4777.

RASFinder™
Remote Access Device

Glossary of Terms

MultiTech® Systems

A

Access: The T1 line element made up of two pairs of wire that the phone company brings to the customer premises. The Access portion ends with a connection at the local telco (LEC or RBOC).

Accunet Spectrum of Digital Services (ASDS): The AT&T 56K bps leased (private) line service. Similar to services of MCI and Sprint. ASDS is available in nx56/64K bps, where n=1, 2, 4, 6, 8, 12.

ACK (ACKnowledgement code) (pronounced "ack"): A communications code sent from a receiving modem to a transmitting modem to indicate that it is ready to accept data. It is also used to acknowledge the error-free receipt of transmitted data. Contrast with NAK.

Adaptive Differential Pulse Code Modulation (ADPCM): In multimedia applications, a technique in which pulse code modulation samples are compressed before they are stored on a disk. ADPCM, an extension of the PCM format, is a standard encoding format for storing audio information in a digital format. It reduced storage requirements by storing differences between successive digital samples rather than full values.

Address: A numbered location inside a computer. It's how the computer accesses its resources, like a video card, serial ports, memory, etc.

AMI line coding: One of two common methods of T1 line coding (with B8ZS). AMI line coding places restrictions on user data (B8ZS does not).

Analog signal: A waveform which has amplitude, frequency and phase, and which takes on a range of values between its maximum and minimum points.

Analog Transmission: One of two types of telecommunications which uses an analog signal as a carrier of voice, data, video, etc. An analog signal becomes a carrier when it is modulated by altering its phase, amplitude and frequency to correspond with the source signal. Compare with digital transmission.

Application Program Interface (API): A software module created to allow dissimilar, or incompatible applications programs to transfer information over a communications link. APIs may be simple or complex; they are commonly required to link PC applications with mainframe programs.

ASCII (American Standard Code for Information Interchange) (pronounced "askey"): A binary code for data that is used in communications and in many computers and terminals. The code is used to represent numbers, letters, punctuation and control characters. The basic ASCII code is a 7-bit character set which defines 128 possible characters. The extended ASCII file provides 255 characters.

Asynchronous Transfer Mode (ATM): A very high-speed method of transmission that uses fixed-size cells of 53 bytes to transfer information over fiber; also known as cell relay.

AT Commands: A standard set of commands used to configure various modem parameters, establish connections and disconnect. The "AT" is used to get the "attention" of the modem before the actual command is issued.

Availability: The measure of the time during which a circuit is ready for use; the complement of circuit "outage" (100% minus % outage = % available).

B

B7ZS (Bipolar 7 Zero Suppression) line coding: One method of T1 line coding (see also "B8ZS" and "AMI"). B7ZS line coding does not place restrictions on user data (AMI does).

B8ZS (Bipolar 8 Zero Suppression) line coding: One of two common methods of T1 line coding (with AMI). B8ZS line coding does not place restrictions on user data (AMI does). A coding method used to produce 64K bps "clear" transmission. (See also "B7ZS" and "AMI" line coding)

Backbone: 1. A set of nodes and their interconnecting links providing the primary data path across a network. 2. In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges. A backbone may be configured as a bus or as a ring. 3. In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected. 4. A common distribution core that provides all electrical power, gases, chemicals, and other services to the sectors of an automated wafer processing system.

Background: An activity that takes place in the PC while you are running another application. In other words, the active user interface does not correspond to the 'background' task.

Bandwidth: The transmission capacity of a computer channel, communications line or bus. It is expressed in cycles per second (hertz), the bandwidth being the difference between the lowest and highest frequencies transmitted. The range of usable frequencies that a transmission medium will pass without unacceptable attenuation or distortion. Bandwidth is a factor in determining the amount of information and the speed at which a medium can transmit data or other information.

Backward Explicit Congestion Notification (BECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiated in the opposite direction of the received frame. See also FECN (Forward Explicit Congestion Notification).

Basic Rate Interface (BRI): An ISDN access interface type comprised of two B-channels each at 64K bps and one D-channel at 64K bps (2B+D).

Bell Operating Companies (BOC): The family of corporations created during the divestiture of AT&T. BOCs are independent companies which service a specific region of the US. Also called Regional Bell Operating Companies (RBOCs).

Bell Pub 41450: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Bell Pub 62310: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Binary Synchronous Communication (BSC): A form of telecommunication line control that uses a standard set of transmission control characters and control character sequences, for binary synchronous transmission of binary-coded data between stations.

Bit (Binary digIT): A bit is the basis of the binary number system. It can take the value of 1 or 0. Bits are generally recognized as the electrical charge generated or stored by a computer that represent some portion of usable information.

Bit Error Rate Test (BERT): A device or routine that measures the quality of data transmission. A known bit pattern is transmitted, and the errors received are counted and a BER (bit error rate) is calculated. The BER is the ratio of received bits in error relative to the total number of bits received, expressed in a power of 10.

Bit robbing: The use of the least significant bit per channel in every sixth frame for signaling. The line signal bits “robbed” from the speech part conveys sufficient pre-ISDN telephony signaling information with the remaining line signal bits providing sufficient line signaling bits for recreating the original sound. See “robbed bit signaling”.

Blue Alarm: An error indication signal consisting of all 1s indicating disconnection or attached device failure. Contrast “Red Alarm” and “Yellow Alarm”.

Bps (bits per second): A unit to measure the speed at which data bits can be transmitted or received. Bps differs from baud when more than one bit is represented by a single cycle of the carrier.

Bridges: 1. A functional unit that interconnects two local area networks that use the same logical link protocol but may use different medium access control protocols. 2. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address. 3. In the connection of local loops, channels, or rings, the equipment and techniques used to match circuits and to facilitate accurate data transmission.

Buffer: A temporary storage register or Random Access Memory (RAM) used in all aspects of data communications which prevents data from being lost due to differences in transmission speed. Keyboards, serial ports, muxes and printers are a few examples of the devices that contain buffers.

Bus: A common channel between hardware devices either internally between components in a computer, or externally between stations in a communications network.

Byte: The unit of information a computer can handle at one time. The most common understanding is that a byte consists of 8 binary digits (bits), because that’s what computers can handle. A byte holds the equivalent of a single character (such as the letter A).

C

Call Setup Time: The time to establish a circuit-switched call between two points. Includes dialing, wait time, and CO/long distance service movement time.

Carrier Group Alarm (CGA): A T1 service alarm generated by a channel bank when an OOF condition occurs for a predefined length of time (usually 300mS to 2.5 seconds). The CGA causes the calls using a trunk to be dropped and for trunk conditioning to be applied.

Carrier signal: An analog signal with known frequency, amplitude and phase characteristics used as a transport facility for useful information. By knowing the original characteristics, a receiver can interpret any changes as modulations, and thereby recover the information.

CCITT (Consultative Committee for International Telephone and Telegraph): An advisory committee created and controlled by the United Nations and headquartered in Geneva whose purpose is to develop and to publish recommendations for worldwide standardization of telecommunications devices. CCITT has developed modem standards that are adapted primarily by PTT (post, telephone and telegraph) organizations that operate phone networks of countries outside of the U.S. See also ITU.

Central Office (CO): The lowest, or most basic level of switching in the PSTN (public switched telephone network). A business PABX or any residential phone connects to the PSTN at a central office.

Centrex: A multi-line service offered by operating telcos which provides, from the telco CO, functions and features comparable to those of a PBX for large business users. See also “Private Branch Exchange”, “Exchange”.

Channel: A data communications path between two computer devices. Can refer to a physical medium (e.g., UTP or coax), or to a specific carrier frequency.

Channel Bank: A device that acts as a converter, taking the digital signal from the T1 line into a phone system and converting it to the analog signals used by the phone system. A channel bank acts as a multiplexer, placing many slow-speed voice or data transactions on a single high-speed link.

CHAP (Challenge-Handshake Authentication Protocol): An authentication method that can be used when connecting to an Internet Service Provider. CHAP allows you to log in to your provider automatically, without the need for a terminal screen. It is more secure than Password Authentication Protocol (See PAP) since it does not send passwords in text format.

Circuit-switched Network: A technology used by the PSTN that allocates a pair of conductors for the exclusive use of one communication path. Circuit switching allows multiple conversations on one talk path only if the end-users multiplex the signals prior to transmission.

Circuit Switching: The temporary connection of two or more communications channels using a fixed, non-shareable path through the network. Users have full use of the circuit until the connection is terminated.

Clear Channel: A transmission path where the full bandwidth is used (i.e., no bandwidth needed for signaling, carrier framing or control bits). A 64K bps digital circuit usually has 8K bps used for signaling. ISDN has two 64K bps circuits, and a 16K bps packet service of which part is used for signaling on the 64K channels.

Client-Server: In TCP/IP, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

Cluster Controller: A device that can control the input/output operations of more than one device connected to it. A cluster controller may be controlled by a program stored and executed in the unit, or it may be entirely controlled by hardware.

Committed Burst Size: The maximum number of bits that the frame relay network agrees to transfer during any measurement interval.

Committed Information Rate (CIR): An agreement a customer makes to use a certain minimum data transmission rate (in bps). The CIR is part of the frame relay service monthly billing, along with actual usage, that users pay to their frame relay service provider.

Compression: 1. The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. 2. In SNA, the replacement of a string of up to 64-repeated characters by an encoded control byte to reduce the length of the data stream to the LU-LU session partner. The encoded control byte is followed by the character that was repeated (unless that character is the prime compression character). 3. In Data Facility Hierarchical Storage Manager, the process of moving data instead of allocated space during migration and recall in order to release unused space. 4. Contrast with decompression.

COMx Port: A serial communications port on a PC.

Congestion: A network condition where there is too much data traffic. The ITU I.233 standard defines congestion managemennt in terms of speed and burstiness.

Congestion Notification: The function in frame relay that ensures that user data transmitted at a rate higher than the CIR are allowed to slow down to the rate of the available network bandwidth.

Consecutive Severely Errored Seconds (CSES): An error condition that occurs when from 3 to 9 SES (Severely Errored Seconds) are logged consecutively.

Customer Premise Equipment (CPE): The generic term for data comm and/or terminal equipment that resides at the user site and is owned by the user with the following exclusions: Over voltage protection equipment, inside wiring, coin operated or pay telephones, “company-official” equipment, mobile telephone equipment, “911” equipment, equipment necessary for the provision of communications for national defense, or multiplexing equipment used to deliver multiple channels to the customer.

D

D4: the T1 4th generation channel bank.

D4 channelization: Refers to the compliance with AT&T TR 62411 for DS1 frame layout.

D4 framing: The T1 format for framing in AT&T D-Series channel banks, in which there are 12 separate 193-bit frames in a super-frame. A D4 framing bit is used to identify the channel and the signaling frame. Signalling for voice channels is carried in-band for every channel, along with the encoded voice. See “robbed-bit signaling”.

Data Communications Equipment (DCE): Any device which serves as the portal of entry from the user equipment to a telecommunications facility. A modem is a DCE for the telephone network (PSTN) that is commonly on site at the user’s premises. Packet Switched Networks have another level of DCE which is most often located at a central office.

Data Link Connection Identifier (DLCI): One of the six components of a frame relay frame. Its purpose is to distinguish separate virtual circuits across each access connection. Data coming into a frame relay node is thus allowed to be sent

across the interface to the specified “address”. The DLCI is confirmed and relayed to its destination, or if the specification is in error, the frame is discarded.

Data Terminal Ready (DTR): A control signal sent from the DTE to the DCE that indicates that the DTE is powered on and ready to communicate.

Dataphone Digital Service (DDS): A private line digital service that offers 2400, 4800, 9600 and 56K bps data rates on an inter-LATA basis by AT&T and on an intra-LATA basis by the BOCs.

Data Service Unit (DSU): A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

Dedicated Line: A communication line that is not switched. The term leased line is more common.

Default: This is a preset value or option in software packages, or in hardware configuration, that is used unless you specify otherwise.

Device driver: Software that controls how a computer communicates with a device, such as a printer or mouse.

Digital Cross-connect System (DCS): The CO device which splits and redistributes the T1 bandwidth. the DCS takes time slots from various T1 lines and alters them to provide the needed connectivity. DCS connections are made with software at an administrator’s workstation.

Digital Data: Information represented by discrete values or conditions (contrast “Analog Data”).

Digital Loopback: A technique used for testing the circuitry of a communications device. Can be initiated locally, or remotely (via a telecommunications device). The tested device decodes and encodes a received test message, then echoes the message back. The results are compared with the original message to determine if corruption occurred en route.

Digital PBX: A Private Branch Exchange that operates internally on digital signals. See also “Exchange”.

Digital Service, level 0 (DS0): The worldwide standard speed (64 Kbps) for digital voice conversation using PCM (pulse coded modulation).

Digital Service, level 1 (DS1): The 1.544 Mbps voice standard (derived from an older Bell System standard) for digitized voice transmission in North America. The 1.544 Mbps consists of 24 digitally-encoded 64 Kbps voice channels (north America) and 2.048 Mbps (30 channels) elsewhere.

Digital Signal: A discrete or discontinuous signal (e.g., a sequence of voltage pulses). Digital devices, such as terminals and computers, transmit data as a series of electrical pulses which have discrete jumps rather than gradual changes.

Digital Signaling Rates (DSn): A hierarchical system for transmission rates, where “DS0” is 64K bps (equivalent to ISDN B channel), and DS1 is 1.5 Mbps (equivalent to ISDN PRI).

Digital Transmission: A method of electronic information transmission common between computers and other digital devices. Analog signals are waveforms: a combination of many possible voltages. A computer’s digital signal may be only “high” or “low” at any given time. Therefore, digital signals may be “cleaned up” (noise and distortion removed) and amplified during transmission.

Digitize: To convert an analog signal to a digital signal.

DIP switch (pronounced “dip switch”): A set of tiny toggle switches, built into a DIP (dual in-line package), used for setting configurable parameters on a PCB (printed circuit board).

Domain Name Server (DNS): Also known as “resolvers”, are a system of computers which convert domain names into IP addresses, which consist of a string of four numbers up to three digits each. Each applicant for a domain name must provide both a primary and a secondary DNS server; a domain name which fails to provide both primary and secondary DNS servers is known as a “lame delegation.”

Driver: A software module that interfaces between the Operating System and a specific hardware device (e.g., color monitors, printers, hard disks, etc.). Also known as a device driver.

Drop and Insert: The process where a portion of information carried in a transmission system is demodulated (“Dropped”) at an intermediate point and different information is included (“Inserted”) for subsequent transmission.

DTE (Data Terminal Equipment): A term used to include any device in a network which generates, stores or displays user information. DTE is a telecommunications term which usually refers to PCs, terminals, printers, etc.

DTMF (Dual-Tone MultiFrequency): A generic push-button concept made popular by AT&T TouchTone.

Dynamic Host Configuration Protocol (DHCP): An IETF protocol which allows a server to dynamically assign IP addresses to Nodes (workstations). DHCP supports manual, automatic and dynamic address assignment; provides client information including the subnetwork mask, gateway address; and is routable. A DHCP server, generally a dedicated server, verifies the device’s indentity, “leases” an IP address for a predetermined period of time and reclaims the address upon expiration for reassignment to another workstation.

E

E&M: A telephony trunking system used for either switch-to-switch, or switch-to-network, or computer/telephone system-to-switch connection.

EIA: The Electronics Industries Association is a trade organization in Washington, DC that sets standards for use of its member companies. (See RS-232, RS-422, RS530.)

Encapsulation: A technique used by network-layer protocols in which a layer adds header information to the protocol data unit from the preceding layer. Also used in “enveloping” one protocol inside another for transmission. For example, IP inside IPX.

Errored Seconds (ES): Any second of operation that all 1.544M bits are not received exactly as transmitted. Contrast “Error Free Seconds”.

Error Free Seconds (EFS): Any second of operation that all 1.544M bits are received exactly as transmitted. Contrast “Errored Seconds”.

ESF Error Event: A T1 error condition that is logged when a CRC-6 error or an out-of-frame (OOF) error occurs.

Ethernet: A 10-megabit baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and transmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

Excess Zeros: A T1 error condition that is logged when more than 15 consecutive 0s or fewer than one 1 bit in 16 bits occurs.

Exchange: A unit (public or private) that can consist of one or more central offices established to serve a specified area. An exchange typically has a single rate of charges (tariffs) that has previously been approved by a regulatory group.

Exchange Area: A geographical area with a single uniform set of charges (tariffs), approved by a regulatory group, for telephone services. Calls between any two points within an exchange area are local calls. See also “Digital PBX”, “PBX”.

Exchange Termination (ET): The carrier’s local exchange switch. Contrast with “Loop Termination - LT”.

Explicit Congestion Management: The method used in frame relay to notify the terminal equipment that the network is overly busy. The use of FECN and BECN is called explicit congestion management. Some end-to-end protocols use FECN or BECN, but usually not both options together. With this method, a congestion condition is identified and fixed before it becomes critical. Contrast with “implicit congestion”.

Extended Super Frame (ESF): One of two popular formats for framing bits on a T1 line. ESF framing has a 24-frame super-frame, where robbed bit signaling is inserted in the LSB (bit 8 of the DS-0 byte) of frames 6, 12, 18 and 24. ESF has more T1 error measurement capabilities than D4 framing. Both ESF and B8ZS are typically offered to provide clear channel service.

F

Failed Seconds: A test parameter where the circuit is unavailable for one full second.

Failed Signal: A T1 test parameter logged when there are more than 9 SES (Severely Errored Seconds).

Fax (facsimile): Refers to the bit-mapped rendition of a graphics-oriented document (fax) or to the electronic transmission of the image over telephone lines (faxing). Fax transmission differs from data transmission in that the former is a bit-mapped approximation of a graphical document and, therefore, cannot be accurately interpreted according to any character code.

Firmware: A category of memory chips that hold their content without electrical power, they include ROM, PROM, EPROM and EEPROM technologies. Firmware becomes “hard software” when holding program code.

Foreground: The application program currently running on and in control of the PC screen and keyboard. The area of the screen that occupies the active window. Compare with “background”.

Fractional T1 (FT1): A digital data transmission rate between 56K bps (DS0 rate) and 1.544M bps (the full T1 rate - in North America). FT1 is typically provided on 4-wire (two copper pairs) UTP. Often used for video conferencing, imaging and LAN interconnection due to its low cost and relatively high speed. FT1 rates are offered in 64K bps multiples, usually up to 768K bps.

Frequency: A characteristic of an electrical or electronic signal which describes the periodic recurrence of cycles. Frequency is inversely proportional to the wavelength or pulse width of the signal (i.e., long wavelength signals have low frequencies and short wavelength signals yield high frequencies).

Foreign Exchange (FX): A CO trunk with access to a distant CO, allowing ease of access and flat-rate calls anywhere in the foreign exchange area.

Foreign Exchange Office (FXO): provides local telephone service from a CO outside of (“foreign” to) the subscriber’s exchange area. In simple form, a user can pick up the phone in one city and receive a tone in the foreign city. Connecting a POTS telephone to a computer telephony system via a T1 link requires a channel bank configured for the FX connection. To generate a call from the POTS set to the computer telephony system, a FXO connection must be configured.

Foreign Exchange Station (FXS): See FX, FXO. To generate a call from the computer telephony system to the POTS set, an FXS connection must be configured.

Forward Explicit Congestion Notification (FECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiatedin the same direction of the received frame. See also BECN (Backward Explicit Congestion Notification).

Frame: A group of data bits in a specific format to help network equipment recognize what the bits mean and how to process them. The bits are sent serially, with a flag at each end signifying the start and end of the frame.

Frame Relay: A form of packet switching that uses small packets and that requires less error checking than other forms of packet switching. Frame relay is effective for sending “bursty” data at high speeds (56/64K, 256K, and 1024K bps) over wide area networks. Frame Relay specifications are defined by ANSI documents ANSI T1.602, T1.606, T1S1/90-175, T1S1/90-213, and T1S1/90-214. In using frame relay, blocks of information (frames) are passed across a digital network interface using a “connection number” that is applied to each frame to distinguish between individual frames.

Frame Relay Forum: A non-profit organization of 300+ vendors and service providers, based in Foster City, CA, that are developing and deploying frame relay equipment.

Frame Relay Implementors Forum: A group of companies supporting a common specification for frame relay connection to link customer premises equipment to telco network equipment. Their specification supports ANSI frame relay specs and defines extensions such as local management.

Frame Relay Access Device (FRAD): A piece of equipment that acts as a concentrator or frame assembler/dissassember that can support multiple protocols and provide basic “routing” functions.

G

Gateway: 1. A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. 2. A network that connects hosts.

Graphical User Interface (GUI): A type of computer interface consisting of a visual metaphor of a real-world scene, often of a desktop. Within that scene are icons, representing actual objects, that the user can access and manipulate with a pointing device.

H

Handshaking: A process that two modems go through at the time of call setup to establish synchronization over the data communications link. It is a synchronization and negotiation process accomplished by the exchange of predefined, mutually recognized control codes.

Hexadecimal: A base 16 numbering system used to represent binary values. Hex uses the numbers 0-9 and the letters A-F: usually notated by an “h” (e.g., “4CF h”, read “four charley fox, hex”). The result is that one hex digit represents a 4-bit value.

High-level Data Link Control (HDLC): An ISO standard, bit-oriented data communications protocol that provides nearly error-free data transfers.

I

Implicit congestion management: A method of informing the terminal that the network is busy. This method relies on the end-system protocol to detect and fix the congestion problem. (TCP/IP is an example of a protocol using only implicit congestion management.) See also “explicit congestion management”.

In-band: Refers to the type of signalling over the conversion path on an ISDN call. Contrast “out-of-band”.

Insufficient Ones: A T1 error condition that is logged when fewer than one 1 in 16 0s or less than 12.5 % average 1s density is received.

Inter Exchange Carrier (IEC): The long distance company (LE) who’s central office provides the point of reference for T1 access. Any common carrier authorized by the FCC to carry customer transmissions between LATAs.

Internet: Refers to the computer network of many millions of university, government and private users around the world. Each user has a unique Internet Address.

Internet Address (IP Address): A unique 32-bit address for a specific TCP/IP host on a network. Normally printed in dotted decimal format (e.g., 129.128.44.227).

Internet Protocol (IP): A protocol used to route data from its source to its destination in an Internet enviroment. The Internet Protocol was designed to connect local area networks. Although there are many protocols that do this, IP refers to the global system of interconnecting computers. It is a highly distributed protocol (each machine only worries about sending data to the next step in the route).

Internetwork Packet Exchange (IPX): A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another. An IPX packet can occasionally get lost when crossing networks, thus IPX does not guarantee delivery of a complete message. Either the application has to provide that control, or NetWare's SPX protocol must be used.

Interoperable: Devices from different vendors that can exchange information using a standard's base protocol.

I/O Addresses: Locations within the I/O address space of your computer used by a device, such as an expansion card, a serial port, or an internal modem. The address is used for communication between software and a device.

IRQ Level (Interrupt Request Level): The notification a processor receives when another portion of the computer's hardware requires its attention. IRQs are numbered so that the device issuing the IRQ can be identified, and so IRQs can be prioritized.

ISA (Industry Standards Architecture) (pronounced "ice a"): The classic 8 or 16-bit architecture introduced with IBM's PC-AT computer.

ISDN (Integrated Services Digital Network): An International telecommunications standard for transmitting voice, video and data over a digital communications line. ISDN is a world-wide telecommunications service that uses digital transmission and switching technology to support voice and digital data communications. Frame relay was partially based on ISDN's data link layer protocol (LAPD). Frame relay can be used to transmit across ISDN services offering circuit-switched connection at 64K bps and higher speeds. Contrast Public Switched Telephone Network (PSTN).

ITU-TSS (formerly CCITT): International Telecommunications Union-Telecommunications Sector; the United Nations organization that prepares standards ("Recommendations") for resolving communications issues and problems.

J

No Entries.

K

Key Telephone System (KTS): Phone devices with multiple buttons that let you select incoming or outgoing CO phone lines directly. Similar in operation to a PBX, except with a KTS you don't have to dial a "9" to call outside the building.

Key Service Unit (KSU): A small device containing the switching electronics for a business key telephone system (KTS).

Key Set: A phone set with several buttons for call holding, line pickup, intercom, autodialing, etc. Also called a touchtone phone (Ericsson) and a KTS (Key Telephone Set).

L

LAPB: Link Access Procedure Balanced; based on the X.25 Layer 2 specification. A full-duplex, point-to-point, bit-synchronous protocol commonly used as a data link control protocol to interface X.25 DTEs. LAPB is the link initialization procedure that establishes and maintains communications between the DTE and the DCE.

LAPD: Link Access Protocol for the D-Channel; based on the ISDN Q.921 specification. A full-duplex point-to-point bit-synchronous link-level protocol for ISDN connections; different from LAPB in its framing sequence. Transmission is in units called "frames", and a frame may contain one or more X.25 packets.

Line Coding: The representation of 1s and 0s on a T1 line. The two methods of line coding commonly used, B8ZS and AMI, differ in the restrictions placed on user data. T1 line coding ensures that sufficient timing information is sent with the digital signal to ensure recovery of all the bits at the far end. Timing information on the T1 line is included in the form of 1s in the data stream; a long string of 0s in the data stream could cause problems recovering the data.

Line Termination (LT): The electronics at the ISDN network side of the user/network interface that complements the NT1 at the user side. The LT and the NT1 together provide the high-speed digital line signals required for BRI access.

Listed Directory Number (LDN): The main number assigned by the telco; the number listed in the phone directory and also provided by Directory Assistance. Some devices can have more than one LDN, such as ISDN devices that have one LDN for voice and another LDN for data.

Local Area Network (LAN): 1. A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. 2. A LAN does not use store-and-forward techniques. 3. A network in which a set of devices are connected to one another for a communication and that can be connected to a larger network.

Local Access and Transport Area (LATA): A post-divestiture geographical area generally equivalent to a Standard Metropolitan Statistical Area. At divestiture, the territory served by the Bell system was divided into approximately 161 LATAs. The Bell Operating Companies (BOCs) provide Intra-LATA services.

Local Exchange Carrier (LEC): The local phone company which provides local (i.e., not long distance) transmission services. AKA “telco”. LECs provide T1 or FT1 access to LDCs (unless the T1 circuit is completely intra-LATA). Inter-LATA T1 circuits are made up of a combination of Access and Long Haul facilities.

Local Management Interface (LMI): A specification for frame relay equipment that defines status information exchange.

Local Loop: A transmission path, typically twisted-pair wire, between an individual subscriber and the nearest public telecommunications network switching center. The wires provide ISDN service, but require an NT1 at the user end and an LT at the network end. (AKA, “loop” or “subscriber loop”.)

Logical Link Control (LLC2): In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. The LLC2 protocol was developed by the IEEE 802 commitee and is common to all LAN standards.

Logical Unit (LU): A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

Long Haul: The T1 element that connects to the Access portion of the long distance company’s (LDC’s) central office. The LDC is commonly called the point of presence (POP). Each LDC has a number of POPs, located throughout the country. The LDC is also called an IEC (Inter Exchange Carrier).

Long Haul Communications: The type of phone call reaching outside of a local exchange (LE).

M

Management Information Base (MIB): A database of network management information used by the Common Management Information Protocol (CMIP) and the Simple Network Management Protocol (SNMP).

Megacom: An AT&T service with a normal WATS line (typically T1) between the customer premise and the AT&T serving class 4 CO are the customer’s responibility.

MegaLink: BellSouth’s leased T1 service.

Message: Associated with such terms as packet, frame, and segment. 1. In information theory, an ordered series of characters intended to convey information. 2. An assembly of characters and sometimes control codes that is transferred as an entry from an originator to one or more recipients.

Modem: A communications device that enables a computer to transmit information over a phone line. It converts the computer’s digital signals into analog signals to send over a phone line and converts them back to digital signals at the receiving end. Modems can be internal and fit into an expansion slot, or external and connect to a serial port.

Multi-Link/PPP (ML/PPP): A ‘bandwidth on demand’ technology that allows one logical PPP connection to add additional channels (as in a second ISDN channel) when the bandwidth is needed (however the vendor defines that situation). It may also be used with leased lines when the total bandwidth needed exceeds the available line speed - a form of inverse muxing.

Multiplexer (Mux): 1. A device that takes several input signals and combines them into a single output signal in such a manner that each of the input signals can be recovered. 2. A device capable of interleaving the events of two or more activities or capable of distributing the events of an interleaved sequence to the respective activities. 3. Putting multiple signals on a single channel.

Multiprotocol: A device that can interoperate with devices utilizing different network protocols.

Multithreading: The ability of a software system to be able to handle more than one transaction concurrently. This is contrasted to the case where a single transaction is accepted and completely processed befor the next transaction processing is started.

N

Nailed Connection: A permanent or dedicated circuit of a previously switched circuit or circuits.

Nailed-up Circuit: A semi-permanent circuit established through a circuit-switching facility for point-to-point connectivity.

NAK (Negative Acknowledgment): Communications code used to indicate that a message was not properly received, or that a terminal does not wish to transmit. Contrast with ACK.

Network: A group of computers connected by cables or other means and using software that enables them to share equipment, such as printers and disk drives to exchange information.

Node: Any point within a network which has been assigned an address.

O

Object-Oriented: A method for structuring programs as hierarchically organized classes describing the data and operations of objects that may interact with other objects.

Office Channel Unit - Data Port (OCU-DP): The CO channel bank used as the interface between the customer's DSU and the channel bank.

Off-hook: The condition of a device which has accessed a phone line (with or without using the line). In modem use, this is equivalent to a phone handset being picked up. Dialing and transmission are allowed, but incoming calls are not answered. Contrast "on-hook".

Off Premise Extension (OPX): An extension or phone that terminates in a location other than that of the PBX. Commonly used to provide a corporate member with an extension of the PBX at home.

Ones Density: the measure of the number of logical 1s on a T1 line compared to a given total number of bits on that line; used for timing information in data recovery in AMI and B8ZS.

On-Hook: The condition of a device which has not accessed a phone line. In modem use, this is equivalent to a telephone handset that has not been picked up. In other words, it can receive an incoming call. Contrast "off-hook".

Open Shortest Path First (OSPF): A hierarchical Interior Gateway Protocol (IGP) routing algorithm for IP that is a proposed standard for the Internet. OSPF incorporates least-cost routing, equal-cost routing, and load balancing.

Outage: The measure of the time during which a circuit is not available for use due to service interrupt. Outage is the complement of circuit "availability" (100% minus % available = % outage).

Out-of-band: Signaling that is separated from the channel carrying the information (e.g., the voice/data/video signal is separate from the carrier signal). Dialing and various other "supervisory" signals are included in the signaling element. Contrast "In-band" signaling.

Out of Frame (OOF): A T1 alarm condition that is logged on the loss of 2, 3 or 4 of 5 consecutive FT framing bits.

P

Packet: 1. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals and, possibly, error control information are arranged in a specific format. 2. Synonymous with data frame. 3. In TCP/IP, the unit of data passed across the interface between the Internet layer and the link layer. A packet includes an IP header and data. A packet can be a complete IP datagram or a fragment of an IP diagram. 4. In X.25, a data transmission information unit. A group of data and control characters, transferred as a unit, determined by the process of transmission. Commonly used data field lengths in packets are 128 or 256 bytes. 5. The field structure and format defined in the CCITT X.25 recommendation.

Packet Assembler/Dissembler (PAD): Used by devices to communicate over X.25 networks by building or stripping X.25 information on or from a packet.

Packet Data: The information format ("packetized") used for packet-mode calls.

Packet Mode: Refers to the switching of chunks of information for different users using statistical multiplexing to send them over the same transmission facility.

Parity bit: An extra bit attached to each byte of synchronous data used to detect errors in transmission.

Password Authentication Protocol (PAP): PAP (and CHAP) are widely-used authentication methods for communicating between RASFinders, both for reaching the Internet and for securing temporary WAN connections such as dial-backup lines. CHAP uses a three-way handshake process that, in concept, resembles a dial-back routine and uses encrypted passwords. With PAP, one RASFinderer connects to the other and sends a plain text login and password.

Permanent Virtual Circuit (PVC): A connection between two endpoints dedicated to a single user. In ISDN, PVCs are establised by network administration and are held for as long as the user subscribes to the service.

Physical Unit (PU): The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only.

Point of Presence (POP): The central office's end points of the long distance carriers.

Point-to-Point Protocol (PPP): A protocol that lets a PC user access TCP/IP (Internet memeber) using an ISDN terminal adapter or a high-speed modem over a standard phone line.

Port: A location for input or output data exchange. Computers, muxes, etc. have ports for various purposes.

Primary Rate Interface (PRI): Used on ISDN. In North America, and Japan, PRI is one 64 Kbps D channel and 23 B channels. Elsewhere, it is one D channel and 30 B channels.

Primitive: An abstract representation of interaction across the access points indicating that information is being passed between the service user and the service provider. The OSI Reference Model defines four types of primitives: Request, Indication, Response and Confirm.

Private Branch Exchange (PBX): A phone exchange located on the customer's premises. The PBX provides a circuit switching facility for phone extension lines within the building, and access to the public phone network. See also "Exchange".

PROM (Programmable Read Only Memory - pronounced "prom"): A permanent memory chip that can be programmed or filled by the customer after by the manufacturer has set initial values. Contrast with ROM.

Protocol: 1. A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. 2. In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. 3. In SNA, the meanings of and the sequencing rules for requests and responses used for managing the network, transferring data, and synchronizing the states of network components. 4. Synonymous with line control discipline.

ProxyServer: A secure gateway that provides multiple LAN users with high performance Internet access by functioning as a TCP/IP proxy server that resides on the outer edge of a firewall.

PSTN (Public Switched Telephone Network): A worldwide public voice telephone network that is used as a telecommunications medium for the transmission of voice, data and other information.

Public Data Network (PDN): A packet-switched network that is available to the public for individual ("subscriber") use. Typically, controlled by a government or a national monopoly.

Public Switched Telephone Network (PSTN): The group of circuit-switching voice carriers, which are commonly used as analog data communications services.

Pulse Code Modulation (PCM): 1. In data communication, variation of a digital signal to represent information; for example, by means of pulse amplitude modulation (PAM), pulse duration modulation (PDM), or pulse position modulation (PPM). 2. Transmissions of analog information in digital form through sampling and encoding the samples with a fixed number of bits.

Pulse dialing: One of two methods of dialing a telephone, usually associated with rotary-dial phones. Compare with "tone dialing".

Q

Quantizing: The process of analog-to-digital conversion by assigning a range, from the contiguous analog values, to a discrete number.

R

Remote Access Dial In User Server (RADIUS): A security feature that uses a single authentication server to centralize security on networks with large modem pools, especially those with multiple communication servers.

Random Access Memory (RAM): A computer's primary workspace. All data must be stored in RAM (even for a short while), before software can use the processor to manipulate the data. Before a PC can do anything useful it must move programs from disk to RAM. When you turn it off, all information in RAM is lost.

RASFinder: A secure gateway that provides multiple LAN users with high performance Internet access by functioning as a TCP/IP RASFinder that resides on the outer edge of a firewall.

Rate Enforcement: The concept in frame relay where frames sent faster than the CIR are to be carried only if the bandwidth is available, otherwise they are to be discarded. (The frame relay network assumes that anything exceeding the CIR is of low priority.) Rate enforcement makes sure that the network will not get so congested that it isn't able to meet the agreed on CIR.

Recognized Private Operating Agency (RPOA): A corporation, private or government-controlled, that provides telecommunications services. RPOAs, such as AT&T, participate as non-voting members in the CCITT.

Red Alarm: A T1 error condition generated when a local failure (e.g., loss of synchronization) exists for 2.5 seconds, causing a Carrier Group Alarm (CGA). See also "Blue Alarm" and "Yellow Alarm".

Request for Comment (RFC): A set of papers in which Internet standards (published and proposed), along with generally-accepted ideas, proposals, research results, etc. are published.

Ring Down Box: A device that emulates a CO by generating POTS calls for testing and product demos.

Ring Down Circuit: A tie line connecting phones where picking up one phone automatically rings another phone. A feature used for emergencies to alert the person at the other phone of the incoming call.

RJ-11: An industry standard interface used for connecting a telephone to a modular wall outlet; comes in 4-and 6-wire packages.

RJ-45: An 8-wire modular connector for voice and data circuits.

Robbed Bit Signaling: The popular T1 signaling mechanism where the A and B bits are sent by each side of the T1 termination and are “buried” in the voice data of each voice channel in the T1 circuit. Since the bits are “robbed” infrequently, voice quality remains relatively uncompromised. See “bit robbing”. The robbed-bit signaling technique is used in D4 channel banks to convey signaling information. The eighth (least significant) bit of each of the 24 8-bit time slots is “robbed” every sixth frame to convey voice-related signaling information such as on-hook, off-hook, etc, for each channel.

Router: A device that connects two networks using the same networking protocol. It operates at the Network Layer (Layer 3) of the OSI model for forwarding decisions.

Routing Information Protocol (RIP): A distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

RS232-C: An EIA standard for a serial interface between computers and peripheral devices (modem, mouse, etc.). It uses a 25-pin DB-25, or a 9-pin DB-9 connector. The RS-232 standard defines the purposes, electrical characteristics and timing of the signals for each of the 25 lines.

RS-422: The EIA standard for a balanced interface with no accompanying physical connector. RS-422 products can use screw terminals, DB9, various DB25, and DB37 connectors.

RS-530: The EIA standard for the mechanical/electrical interface between DCEs and DTEs transmitting synchronous or asynchronous serial binary data. RS-530 provides for high data rates with the same connector used for RS-232; however, it is incompatible with RS-232.

S

Serial Port: The connector on a PC used to attach serial devices (those that need to receive data one bit after another), such as a mouse, a printer or a modem. This consists of a 9- or 25-pin connector that sends data in sequence (bit by bit). Serial ports are referred to as “COMx” ports, where x is 1 to 4 (i.e., COM1 through COM4). A serial port contains a conversion chip called a “UART” which translates between internal parallel and external serial formats.

Serial Line Internet Protocol (SLIP): An Internet protocol which is used to run IP over serial lines such as telephone circuits.

Service: The requirements offered by an RPOA to its customers to satisfy specific telecommunications needs.

Severely Errored Seconds (SES): Refers to a typical T1 error event where an error burst occurs (a short term, high bit-error rate that is self-clearing). Per the ITU-T (CCITT) G.821: any second in which the BER is less than 1x10 -3 .

Signaling: The process of establishing, maintaining, accounting for, and terminating a connection between two endpoints (e.g., the user premises and the telco CO). Central office signals to the user premises can include ringing, dial tone, speech signals, etc. Signals from the user’s telephone can include off-hook, dialing, speech to far-end party, and on-hook signals. In-band signaling techniques include pulse and tone dialing. With common channel signaling, information is carried out-of-band.

Simple Network Management Protocol (SNMP): TCP/IP protocol that allows network management.

Simple Network Time Protocol (SNTP): A protocol used to allow network access to accurate clocks and other sources of time-based information.

Simultaneous Voice Data (SVD): A technology for letting a user send data via a modem, and use a handset to talk to another user at the same time over the same connection. The alternative, making a second call, can be expensive or even impossible. The uses for SVD are telecommuting, videoconferencing, distant learning, tech support, etc.

Stop Bit: One of the variables used for timing in asynchronous data transmission. Depending on the devices, each character may be trailed by 1, 1.5, or 2 stop bits.

Superframe (D4): A T1 transmission format that consists of 12 DS1 frames, or 2316 bits. A DS1 frame consists of 193 bit positions. A frame overhead bit is in the first position, and it is used for frame and signaling phase alignment only.

Subscriber Loop: See “Local loop”.

Switched 56: A circuit-switched (full duplex digital synchronous data transmission) service that lets you dial a number and transmit data to it at 56K bps. It is a relatively low cost service, widely used in North America for telecommuting, videoconferencing and high speed data transfers. Many phone companies are (or will be) phasing out Switched 56 in favor of ISDN service.

Switched Virtual Circuit (SVC): A type of data transmission where the connection is maintained only until the call is cleared.

Switched Line: In communications, a physical channel established by dynamically connecting one or more discrete segments. This connection lasts for the duration of the call, after which each segment can be used as part of a different channel. Contrast with leased line.

Switched Network: A network in which a temporary connection is established from one point via one or more segments.

Synchronous Data Link Control (SDLC): A discipline conforming to subsets of the Advanced Data Communications Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex, or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop.

Synchronous Transmission: The transmission of data which involves sending a group of characters in a packet. This is a common method of transmission between computers on a network or between modems. One or more synchronous characters are transmitted to confirm clocking before each packet of data is transmitted. Compare to Asynchronous Transmission.

Systems Network Architecture (SNA): The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks.

T

Tariff: The rate/availability schedule for telephone and ISDN services from a regulated service provider.

TCP/IP: A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

T Carrier: The generic name for a digitally multiplexed carrier system. In the North American digital hierarchy, a T is used to designate a DS (digital signal) level hierarchy. Examples: T1 (DS1) is a 1.544 M bps 24-channel designation. In Europe, T1 is called E1. The T Carrier system was originally designed for transmitting digitized voice signals, but has since been adapted for digital data applications.

T1: A digital transmission link capable of 1.544M bps. T1 uses two pairs of normal UTP, and can handle 24 voice conversations, each digitized at 64K bps. T1 is a standard for digital transmission in the U.S., Canada, Japan and Hong Kong. T1 is the access method for high-speed services such as ATM, frame relay, and SMDS. See also T Carrier, T1 line and FT1.

T1 Channel Tests: A set of diagnostics that vary by carrier, used to verify a T1 channel operation. Can include Tone, Noise Level, Impulse Noise Level, Echo Cancelers, Gain, and Crosstalk testing.

T1 Framing: To digitize and encode analog voice signals requires 8000 samples per second (twice the highest voice frequency of 4000 Hz). Encoding in an 8-bit word provides the basic T1 block of 64K bps for voice transmission. This “Level 0 Signal, as its called, is represented by “DS-0”, or Digital Signal at Level 0. 24 of these voice channels are combined into a serial bit stream (using TDM), on a frame-by-frame basis. A frame is a sample of all 24 channels; so adding in a framing bit gives a block of 193 bits (24x8+1=193). Frames are transmitted at 8000 per second (the required sample rate), creating a 1.544M (8000x193=1.544M) transmission rate.

T1 Line: A digital communications facility that functions as a 24-channel pathway for data or voice transmission. A T1 line is composed of two separate elements: the Access element and the Long Haul element.

T1 Mux: A device used to carry many sources of data on a T1 line. The T1 mux assigns each data source to distinct DS0 time slots within the T1 signal. Wide bandwidth signals take more than one time slot. Normal voice traffic or 56/64K bps data channels take one time slot. The T1 mux may use an internal or external T1 DSU; a “channel bank” device typically uses an external T1 CSU.

Transmission Control Protocol / Internet Program (TCP/IP): A multi-layer set of protocols developed by the US Department of Defense to link dissimilar computers across dissimilar and unreliable LANs.

Terminal: The screen and keyboard device used in a mainframe environment for interactive data entry. Terminals have no “box”, which is to say they have no file storage or processing capabilities.

Terminal Adapter (TA): An ISDN DTE device for connecting a non-ISDN terminal device to the ISDN network. Similar to a protocol converter or an interface converter, a TA connects a non-ISDN device between the R and S interfaces. Typically a PC card.

Tie line: A dedicated circuit linking two points without having to dial a phone number (i.e., the line may be accessed by lifting the telephone handset or by pushing a button).

Time-Division Multiplexing (TDM): Division of a transmission facility into two or more channels by allotting the common channel to several different information channels, one at a time.

Time Slot: One of 24 channels within a T1 line. Each channel has a 64K bps maximum bandwidth. “Time slot” implies the time division multiplexing organization of the T1 signal.

Toll Call: A call to a location outside of your local service area (i.e., a long distance call).

Tone dialing: One of two methods of dialing a telephone, usually associated with Touch-Tone® (push button) phones. Compare with pulse dialing.

Topology: Physical layout of network components (cables, stations, gateways, and hubs). Three basic interconnection topologies are star, ring, and bus networks.

Transmission Control Protocol (TCP): A communications protocol used in Internet and in any network that follows the US Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet protocol is the underlying protocol.

Transport Layer: Layer 4 of the Open Systems Interconnection (OSI) model; provides reliable, end-to-end delivery of data, and detects transmission sequential errors.

Transport Protocol Data Unit (TPDU): A transport header, which is added to every message, contains destination and source addressing information that allows the end-to-end routing of messages in multi-layer NAC networks of high complexity. They are automatically added to messages as they enter the network and can be stripped off before being passed to the host or another device that does not support TPDU's.

Trunk: Transmission links that interconnect switching offices.

TSR (terminate and stay resident): A software program that remains active and in memory after its user interface is closed. Similar to a daemon in UNIX environments.

Tunneling: Encapsulation data in an IP packet for transport across the Internet.

Twisted pair wiring: A type of cabling with one or more pairs of insulated wires wrapped around each other. An inexpensive wiring method used for LAN and telephone applications, also called UTP wiring.

U

UART (Universal Asynchronous Receiver/Transmitter) (pronounced "you art"): A chip that transmits and receives data on the serial port. It converts bytes into serial bits for transmission, and vice versa, and generates and strips the start and stop bits appended to each character.

UNIX: An operating system developed by Bell Laboratories that features multiprogramming in a muti-user environment.

Unshielded Twisted Pair (UTP): Telephone-type wiring. Tansmission media for 10Base-T.

V

V.25bis: An ITU-T standard for synchronous communications between a mainframe or host and a modem using HDLC or other character-oriented protocol.

V.54: The ITU-T standard for local and remote loopback tests in modems, DCEs and DTEs. The four basic tests are:

- local digital loopback (tests DTE send and receive circuits),
- local analog loopback (tests local modem operation),
- remote analog loopback (tests comm link to the remote modem), and
- remote digital loopback (tests remote modem operation).

Virtual Circuit: A logical connection. Used in packet switching wherin a logical connection is established between two devices at the start of transmission. All information packets follow the same route and arrive in sequence (but do not necessarily carry a complete address).

W

Wide Area Network (WAN): 1. A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. 2. A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. Contrast with local area network (LAN).

Wide Area Telecommunications Service (WATS): A low-cost toll service offered by most long distance and local phone companies. Incoming (800 call service, or IN-WATS) and outgoing WATS are subscribed to separately, but over the same line.

X

X.25: ITU-T's definition of a three-level packet-switching protocol to be used between packet-mode DTEs and network DCEs. X.25 corresponds with layer 3 of the 7-layer OSI model.

Y

Yellow Alarm: An error indication sent by the T1 device when it has not gotten a receive signal, or cannot synchronize on the receive signal received. Contrast "Red Alarm" and "Blue Alarm".

Z

Zero Byte Time Slot Interchange (ZBTSI): A method for allowing 64K bps unrestricted user data (allowing all 0s in the user data). An alternative to (but not as popular as) B8ZS.

Index

A

Adding RAM, MTASR3-200 14
Address filtering 49
Answer command 87
Applications setup 58
Applications, typical
  LAN-to-LAN routing 41
  Remote Access Service (RAS) 35
Archie, defined 95
ASCII String 19
Asynchronous Communications Mode command . 91
AT commands
  %B 92
  %C 92
  &&S 93
  &B 90
  &C 90
  &D 90
  &F 90
  &G 90
  &J 90
  &K 90
  &M 91
  &Q 91
  &S 91
  &T 91
  &V 91
  &W 91
  &Y 91
  &Z= 91
  +++AT<CR> 87
  +ES= 93
  -C 92
  \G 91
  \J 91
  \K 92
  \N 92
  \Q 92
  \V 92
  \X 92
  A 87
  A/ 87
  AT 87
  B 87
  C 87
  E 88
  F 88
  H 88
  L 88
  M 89
  N 89
  O 89
  Q 89
  S= 89
  S? 89
  V 89
  X 89
  Y 90
  Z 90
AT&T's "call card" tones 87, 88
Attention code 87
Attribute values, Radius 37
Authentication 45
Authentication, RIPv2 45
Auto protocols, user permissions 24
Auxiliary Relay Control command 90

B

Back panel, RASFinder 9
Bandwidth optimization 52
Bell 212A mode 87
Blacklist 92
Bonding WAN ports (MLPPP) 42
Break signal 92
Bridging IPX packets 52
Building your remote user database 23

C

Cabling diagrams 81
Cabling Your RASFinder 13
Callback-Delay attribute, Radius 37
Canadian limitations notice 86
Carrier Control command 87
Client Setup 59
Command connector 9
Command port cable 81
Command port specifications 10
Communication Standard command 87
Communications Mode command 91
Configuration
  selecting 91
  storing 91
  viewing 91
Configuration, management menu 73
Configuration Port Setup 33
Configuration Utilities 33
Configuring
  the Modem-Sharing Software 61
Connectors, MTASR3-200 9

D

Data Buffer Control command 91
Data buffering 91
Data Calling Tone command 92
Data Compression Control command 92

Data mode 89
DCD Control command 90
Default settings 90
detect AT&T's "call card" tone 87
DHCP (Dynamic Host Configuration Protocol) 46
Diagnostics, RASFinder 58
Dial Command 87
Dial Stored Telephone Number Command 88
Dial-out, RASFinder management 73
DNS 46
DNS, defined 95
DSR Control command 91
DTR Control command 90

E

Echo Command Mode Characters command 88
Echo Online Data Characters command 88
Electrical/Physical specifications 10
EMC, Safety and Terminal Directive Compliance .. 86
Enable Synchronous Buffered Mode command 93
ENTER key 87
Error Correction Mode Selection command 92
Escape sequence 87
Ethernet 10Base-T connector 9
Ethernet LEDs, defined 8
Ethernet port, configuation 44
Ethernet port specifications 10

F

Fail LED, defined 8
Fallback 89
Fax branding statement 84
FCC Part 15 statement 84
FCC Part 68 Telecom statement 85
File Transfer Protocol, defined 95
Filtering, IPX packets 53
Filtering, remote user database 26
Filtering, spanning tree 54
Filtering, user permissions 26
Filters, RASFinder 49
Finger, defined 95
Flow control 90, 91, 92
Frame type, Ethernet configuration 44
Front panel, RASFinder 8

G

Gopher, defined 95
Guard tone 90

H

H.324 93
Handshake 89
Hanging up 87, 88
Hook Control command 88
HTML, defined 95
HTTP, defined 95

I

ICMP filtering 50
ICMP packet types 50
Inactivity Timer 92
Inbound user service type attribute, Radius 37
Information Request Command 88
Information Request Commands 88
Internet addresses 79
Internet Protocol, defined 96
IP port setup 44
IPX virtual port setup 51

L

LAN cables 81
LAN-based remote configuration 70
LAN-to-LAN routing 41
LED display 8
Limited Warranty
  On-line Warranty Registration 77
Link connectors 9
Load Factory Default Settings command 90
Local Flow Control Selection command 90, 92
Long Space Disconnect command 90

M

Management, management menu 73
MNP 5 data compression 92
MNP error correction 92
Modem Port Flow Control command 91
Modem Reset command 90
Modem-based remote configuration 68
Modulation Handshake command 89
Monitor Speaker Mode command 89
Monitor Speaker Volume command 88
MTASR3-200
  Adding RAM (Optional) 14
  Back panel 9
  Cabling 13
  Cabling diagrams 81
  Configuration 34
  Front panel 8
  Overview 6
  Program group 33
  RAS Client setup 59
  RAS Dial-out Re-director 61
  RASFinder setup 34
  Remote configuration 68
  Remote management 72
  Specifications 10
  Typical applications 35
  Unpacking 12
  Warranty, service, and tech support 77
Multi-Tech Internet sites 79
MultiLink Point-to-Point Protocol setup 42

O

On-hook/off-hook 88
On-line Warranty Registration 77
Online command mode 89
ordering replacement parts 79
OSPF (Open Shortest Path First) 46

P

Ping, defined 95
POP, defined 95
Port filtering 49
Power connector 9
Power LED, defined 8
PPP port setup 57
PPP/SLIP, setup 42
Protocol permissions attribute, Radius 37
Protocol Result Code command 92
ProxyServer Software 33

R

Radius, defined 35
Radius security service 36
RAM, adding 14
RAS application
  Radius, using 35
  Remote User Data Base, using 38
RAS Dial-Out Redirector
  Installing WINMCSI modem-sharing software ... 61
  Overview 61
  Running WINMSCI workstation software 64
Read Register Value command 89
Regulatory information 84
Remote Configuration
  LAN-Based 70
  Modem-Based 68
Remote management
  Overview 72
  Telnet 72
Remote user data base, RAS application 38
Remote user database, management menu 74
Repeat last command 87
replacement parts 79
Resetting the modem 90
Result Code Format command 89
Result Code Selection command 89
Result codes 92
Result Codes Enable/Disable command 89
Retrain 90
Return Online to Data Mode command 89
RIPv2 45
RLogin, auto protocols 24
Roaming-Callback attribute, Radius 37
Router Name 19
Routing Information Protocol 45
Routing Information Protocol (RIP) 44
Routing Information Protocol, Version 2 (RIPv2) ... 45

S

S-registers
  reading 89
  setting 89
Safety Warning Telecom 12
Scripting
  Example script 82
Select Stored Configuration command 91
Self-Test commands 91
Set Break Control command 92
Set Register Value command 89
Setting up WAN ports as client-only 46
Setup Menu
  Spanning Tree Setup 52
  WAN Port Setup 56
Shared secret, Radius 37
Shell user service type attribute, Radius 37
SIMM connector 14
SMTP, defined 95
SNMP, defined 95
Software 33
  Description 33
Spanning tree filtering setup 54
Spanning Tree Setup 52
Speaker Codec Loopback command 93
Speaker, controlling 88, 89
Specifications, MTASR3-200 10
Speed conversion (data buffer) 91
Static routes, setting up 46
Store Current Configuration command 91
Store Telephone Number command 91
Storing
  telephone numbers 91
Synchronous buffered mode 93

T

TCP/IP 94
Telnet
  Cient 72
  Defined 95
  RASFinder management menu 73
  TCP/IP stack 72
Telnet, auto protocols 24
Testing 91, 93
Testing DSP 56K Code version/Checksum Command 93
Testing External RAM Command 93
Testing DSP 56K Code Version/Checksum 93
Testing External RAM 93
Traceroute, defined 95
Transparent bridging 54

U

Uninstall Proxy Server Configuration 33
Unnumbered Link, WAN ports 45

Unpacking the MTASR3-200 12
User permissions, assigning 39
User permissions, remote user database 24

V

V.22 mode 87
V.22bis Guard Tone command 90
V.25 92
V.32 Auto Retrain command 90
V.42 eror correction 92
V.42bis data compression 92
Video 93
View Current Configuration command 91
View Numbers in Blacklist command 92

W

WAN cables 81
WAN configuration, management menu 74
WAN Device Configuration 33
WAN link specifications 10
WAN port LEDs, defined 8
WAN Port Setup 56
WEB browser management 75
Whois/NICNAME, defined 95
Windows sockets 70
WINMCSI modem-sharing software 61
WINMSCI workstation software 64

X

XON/XOFF Pass-Through command 92